INFORME: VULNERABILIDADES TRIMESTRE 6

SERVICIOS TIC

MINISTERIO DE EDUACIÓN NACIONAL

UNIÓN TEMPORAL GESTIÓN INTEGRAL MEN

Abril de 2022

TABLA DE CONTENIDO

1. OBJETIVO 4

2. ALCANCE 4

3. METODOLOGÍA 4

4. EJECUCIÓN 5

4.1 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN EN CERTIFICACIÓN CON EXCEPCIÓN .5

4.1.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS 5

4.1.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS 7

4.1.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS 12

4.1.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS 21

4.2 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDOR DE BASES DE DATOS - CERTIFICACIÓN 22

4.2.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS 22

4.2.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS 24

4.2.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS 25

4.2.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS 30

4.3 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN PRODUCCIÓN CON EXCEPCIÓN 31

4.3.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS 31

4.3.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS 34

4.3.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS 44

4.3.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS 59

4.4 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDOR DE BASES DE DATOS - PRODUCCIÓN 61

4.4.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS 62

4.4.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS 64

4.4.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS 68

4.4.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS 78

5. RESUMEN EJECUTIVO CRITICIDAD DE LAS VULNERABILIDADES IDENTIFICADAS 80

6. CONCLUSIONES Y RECOMENDACIONES 82

7. ANEXOS 83

TABLA DE ILUSTRACIONES

Ilustración 1. Criticidad de las vulnerabilidades detectadas para los servidores de las aplicaciones seleccionadas del ambiente de certificación con excepción. 80

Ilustración 2. Criticidad de las vulnerabilidades detectadas para los servidores de bases de datos de las aplicaciones seleccionadas del ambiente de certificación. 81

Ilustración 3. Criticidad de las vulnerabilidades detectadas para los servidores de las aplicaciones seleccionadas del ambiente de producción con excepción. 81
Ilustración 4. Criticidad de las vulnerabilidades detectadas para los servidores de bases de datos de las aplicaciones seleccionadas del ambiente de producción. 82

ÍNDICE DE TABLAS

Tabla 1. Vulnerabilidades críticas sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre. 7
Tabla 2. Vulnerabilidades Altas sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre 11
Tabla 3. Vulnerabilidades Medias sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre. 21
Tabla 4. Vulnerabilidades Bajas sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre. 22
Tabla 5. Vulnerabilidades Críticas sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre. 23
Tabla 6. Vulnerabilidades Altas sobre IP servidores de bases de datos de certificación de los sistemas definidos para el 6to trimestre. 25
Tabla 7. Vulnerabilidades Medias sobre IP servidores de bases de datos de certificación de los sistemas definidos para el 6to trimestre. 30
Tabla 8. Vulnerabilidades Bajas sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre. 31
Tabla 9. Vulnerabilidades Críticas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre. 34
Tabla 10. Vulnerabilidades Altas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre. 43
Tabla 11. Vulnerabilidades Medias sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre. 59
Tabla 12. Vulnerabilidades Bajas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre. 61
Tabla 13. Vulnerabilidades Críticas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre. 64
Tabla 14. Vulnerabilidades Altas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre. 68
Tabla 15. Vulnerabilidades Medias sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre. 78
Tabla 16. Vulnerabilidades Bajas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre. 80

1. OBJETIVO

Presentar el resultado del escaneo y análisis de vulnerabilidades realizado durante la primera semana del mes de abril del 2022 que corresponde a lo acordado para el sexto trimestre de acuerdo con el plan de seguridad, sobre las Aplicaciones del Ministerio de Educación Nacional registradas en el inventario de aplicaciones en su versión 114 que corresponde a la versión más reciente en el momento de presentar el RFC que sustenta el escaneo de vulnerabilidades.

2. ALCANCE

El presente informe muestra el resultado de un escaneo de vulnerabilidades ejecutado sobre la infraestructura que soporta las aplicaciones registradas en el inventario de aplicaciones del Ministerio de Educación Nacional para sus ambientes de certificación y de producción. Para su selección, se tomó como referencia la versión más reciente del inventario que para la fecha en el que se presentó el RFC_10471_OC63260 para ejecución del escaneo, correspondía a la versión 114 del inventario de aplicaciones. Estos sistemas se relacionan en la hoja "Sistemas" del archivo anexo "Sistemas_Trimestre_6.xlsx", en donde se aclara además si la aplicación cuenta con ambiente de certificación y producción.

Hay sistemas en los que el inventario de aplicaciones no registra información de su infraestructura y solo registra el código de aplicación y nombre y/o código. Esos casos son los que corresponden a aquellos sistemas que aparecen sin ambiente de producción ni certificación en la tabla de la hoja "Sistemas".

3. METODOLOGÍA

Una vez definido el alcance, se procedió a obtener las IPs que soportan el servicio de las aplicaciones. A cada aplicación se le realizará un escaneo de vulnerabilidades a nivel de servidor(es) de aplicación y servidor(es) de bases de datos en su respectivo ambiente.

Los datos correspondientes a las IPs que serán objeto del escaneo se pueden verificar en la hoja "Infraestructura Sistemas" del archivo anexo "Sistemas_Trimestre_6.xlsx" en las columnas D, E, F y G. Así que una vez identificadas las IPs se procedió a ejecutar el escaneo de vulnerabilidades. Este proceso se realizó utilizando el software Nessus, el cual se encuentra instalado en un equipo físico de la Unión Temporal que cuenta con una comunicación a la infraestructura del ministerio.

La cantidad de vulnerabilidades detectadas por cada IP se discriminan por criticidad y se registran en las tablas de los apartados de situación actual de vulnerabilidades de cada escenario evaluado sobre la fila correspondiente al código de aplicación a la que pertenece el servidor correspondiente. Posteriormente, se registran análisis y recomendaciones por cada vulnerabilidad encontrada en cada escenario, relacionando el código de la aplicación en la que fue detectada.

El análisis se realizó sin usuario autenticado y sin vectores de evaluación que generaran denegación de servicio. La calificación de las vulnerabilidades se realizó directamente por la herramienta de escaneo de vulnerabilidades. De igual manera, el insumo para la mitigación de vulnerabilidades es el mismo reporte de la herramienta Nessus la cual indica la descripción y posible solución de cada una de ellas.

4. EJECUCIÓN

Los escaneos realizados se dividieron en 4 escenarios y sus resultados son mostrados de la siguiente forma:

- Escaneo de Vulnerabilidades a Servidor de Aplicación Certificación: Escaneo a las IPs de los servidores en los que están soportadas las aplicaciones en el ambiente de certificación.
- Escaneo de Vulnerabilidades a Servidor de Bases de Datos de Certificación: Escaneo a las IPs de los servidores en los que están las bases de datos de las aplicaciones en el ambiente de certificación.
- Escaneo de Vulnerabilidades a Servidor de Aplicación Producción: Escaneo a las IPs de los servidores en los que están soportadas las aplicaciones en el ambiente de producción.
- Escaneo de Vulnerabilidades a Servidor de Bases de Datos de Producción: Escaneo a las IPs de los servidores en los que están las bases de datos de las aplicaciones del ambiente de producción.

4.1 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN EN CERTIFICACIÓN CON EXCEPCIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “D” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_6.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Certificación-App” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas de acuerdo con la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja.

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.1.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico
Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.

Código Aplicaciones Afectadas	APP255, APP272, APP281, APP235, APP241, APP017, APP025, APP114, APP157

Vulnerabilidad	Oracle Database Multiple Vulnerabilities (April 2013 CPU)
Riesgo	Crítico
Descripción	El servidor de base de datos de Oracle remoto le falta la Actualización crítica del parche (CPU) de abril de 2013 y, por lo tanto, está potencialmente afectado por problemas de seguridad en los siguientes componentes: - Workload Manager - Network Layer
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de abril de 2013.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad	Oracle Database Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de Oracle Database que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle Database que sea compatible actualmente.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad	Oracle GlassFish Server 3.1.2.x < 3.1.2.15 Multiple Vulnerabilities (July 2016 CPU)
Riesgo	Crítico
Descripción	Según su número de versión autoinformado, el servidor Oracle GlassFish que se ejecuta en el host remoto es 3.1.2.x anterior a 3.1.2.15.
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.15 o posterior
Código Aplicaciones Afectadas	APP111

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)
Riesgo	Crítico
Descripción	El Oracle WebLogic Server remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS Core en la función readObject() debido a una desinfección incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de una carga útil de objeto manipulado, para eludir la lista negra ClassFilter.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2016.
Código Aplicaciones Afectadas	APP054

Vulnerabilidad	Oracle WebLogic Server RCE (CVE-2020-14882)
Riesgo	Crítico
Descripción	La versión de Oracle WebLogic Server instalada en el host se ve afectada por una vulnerabilidad de ejecución remota de código en el subcomponente Oracle Fusion Middleware Console. Un atacante remoto no autenticado puede aprovechar esto, a través de una solicitud HTTP especialmente diseñada, para ejecutar comandos arbitrarios.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de octubre de 2020 y el aviso de alerta de seguridad de Oracle para CVE-2020-14750.
Código Aplicaciones Afectadas	APP235, APP234

Vulnerabilidad	PHP Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión, la instalación de PHP en el host ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de PHP que sea soportada actualmente.
Código Aplicaciones Afectadas	APP324

Vulnerabilidad	SSL Version 2 and 3 Protocol Detection
Riesgo	Crítico
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. Un atacante puede aprovechar estas fallas para realizar ataques de man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo. NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía sólida" de PCI SSC.
Solución	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior.
Código Aplicaciones Afectadas	APP223

Tabla 1. Vulnerabilidades críticas sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre.

4.1.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad (x7)	- Apache 2.4.x < 2.4.39 Multiple Vulnerabilities - Apache 2.4.x < 2.4.46 Multiple Vulnerabilities - Apache 2.4.x < 2.4.47 Multiple Vulnerabilities - Apache < 2.4.49 Multiple Vulnerabilities - Apache 2.4.x < 2.4.52 Multiple Vulnerabilities - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities - Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
Riesgo	Alto
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache 2.4.53 o posterior.
Código Aplicaciones Afectadas	APP324, APP263

Vulnerabilidad (x7)	- Apache Tomcat 7.0.x < 7.0.52 Content-Type DoS - Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service - Apache Tomcat 7.0.41 < 7.0.90 Multiple Vulnerabilities - Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE) - Apache Tomcat 7.0.0 < 7.0.94 Remote Code Execution Vulnerability (Windows)
Riesgo	Alto
Descripción	El servidor Apache Tomcat se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache Tomcat versión 7.0.100, 8.5.51, 9.0.31 o posterior.
Código Aplicaciones Afectadas	APP223, APP044, APP174

Vulnerabilidad	Apache Tomcat AJP Connector Request Injection (Ghostcat)
Riesgo	Alto
Descripción	Se encontró una vulnerabilidad de lectura/inclusión de archivos en el conector AJP. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para leer archivos de aplicaciones web desde un servidor vulnerable. En los casos en que el servidor vulnerable permite la carga de archivos, un atacante podría cargar código malicioso de JavaServer Pages (JSP) dentro de una variedad de tipos de archivos y obtener la ejecución remota de código (RCE).
Solución	Actualice la configuración de AJP para requerir autorización y / o actualice el servidor Tomcat a 7.0.100, 8.5.51, 9.0.31 o posterior.
Código Aplicaciones Afectadas	APP008, APP087, APP088, APP089, APP241

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.

Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP323, APP257, APP256, APP269

Vulnerabilidad	nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities
Riesgo	Alto
Descripción	Según el encabezado de respuesta del servidor, la versión instalada de nginx es 1.9.5 anterior a 1.16.1 o 1.17.x anterior a 1.17.3. Por lo tanto, se ve afectado por múltiples vulnerabilidades de denegación de servicio: Existe una vulnerabilidad de denegación de servicio en la pila del protocolo HTTP/2 debido al manejo inadecuado de condiciones excepcionales. Un atacante remoto no autenticado puede explotar esto, manipulando el tamaño de la ventana y la prioridad de transmisión de una solicitud de datos de gran tamaño, para provocar una condición de denegación de servicio. (CVE-2019-9511). Existe una vulnerabilidad de denegación de servicio en la pila del protocolo HTTP/2 debido al manejo inadecuado de condiciones excepcionales. Un atacante remoto no autenticado puede explotar esto creando múltiples flujos de solicitudes y barajando continuamente la prioridad de los flujos para causar una condición de denegación de servicio. (CVE-2019-9513). Existe una vulnerabilidad de denegación de servicio en la pila del protocolo HTTP/2 debido al manejo inadecuado de condiciones excepcionales. Un atacante remoto no autenticado puede explotar esto, enviando una secuencia de encabezados con un nombre de encabezado de longitud cero y un valor de encabezado de longitud cero, para provocar una condición de denegación de servicio. (CVE-2019-9516).
Solución	Actualice a la versión nginx 1.16.1/1.17.3 o posterior.
Código Aplicaciones Afectadas	APP310

Vulnerabilidad (x7)	- Oracle Database Multiple Vulnerabilities (January 2011 CPU) - Oracle Database Multiple Vulnerabilities (April 2011 CPU) - Oracle Database Multiple Vulnerabilities (July 2011 CPU) - Oracle Database Multiple Vulnerabilities (October 2011 CPU) - Oracle Database Multiple Vulnerabilities (April 2012 CPU) - Oracle Database Multiple Vulnerabilities (January 2013 CPU) - Oracle Database Multiple Vulnerabilities (July 2013 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad (x2)	- Oracle GlassFish Server 2.1.1.x < 2.1.1.30 / 3.0.1.x < 3.0.1.15 / 3.1.2.x < 3.1.2.16 Multiple Vulnerabilities (January 2017 CPU) - Oracle GlassFish Server 3.0.1.x < 3.0.1.17 / 3.1.2.x < 3.1.2.18 (October 2017 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.

Solución	Actualice a Oracle GlassFish Server versión 3.0.1.17/3.1.2.18 o posterior como se indica en el aviso de actualización de parche crítico de Oracle de octubre de 2017.
Código Aplicaciones Afectadas	APP111

Vulnerabilidad (x4)	- Oracle GlassFish Server Multiple Vulnerabilities (April 2015 CPU) (POODLE) - Oracle GlassFish Server Unspecified Vulnerability (January 2015 CPU) - Oracle GlassFish Server Multiple Vulnerabilities (July 2014 CPU) - Oracle GlassFish Server Multiple Vulnerabilities (July 2015 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP111

Vulnerabilidad	Oracle TNS Listener Remote Poisoning
Riesgo	Alto
Descripción	El listener de Oracle TNS permite el registro de servicios desde un host remoto. Un atacante puede aprovechar este problema para desviar datos de un cliente o servidor de base de datos legítimo a un sistema especificado por el atacante. Los exploits exitosos permitirán al atacante manipular las instancias de la base de datos, lo que potencialmente facilitará ataques de man-in-the-middle, secuestro de sesión o denegación de servicio en un servidor de base de datos legítimo.
Solución	Aplique la solución alternativa en el aviso de Oracle.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad	Oracle WebLogic Java Object Deserialization RCE
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a llamadas de deserializado no seguras de objetos Java no autenticados a la biblioteca Apache Commons Collections (ACC). Un atacante remoto no autenticado puede explotar esto para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Actualice a la versión corregida relevante a la que se hace referencia en el aviso del proveedor.
Código Aplicaciones Afectadas	APP054

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018

Código Aplicaciones Afectadas	APP054, APP235

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a una deserialización no segura de objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2018.
Código Aplicaciones Afectadas	APP054, APP235

Vulnerabilidad (x2)	- Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU) - Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2016.
Código Aplicaciones Afectadas	APP054, APP235

Vulnerabilidad	SNMP Agent Default Community Name (public)
Riesgo	Alto
Descripción	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP remoto. Un atacante puede usar esta información para obtener más conocimiento sobre el host remoto o para cambiar la configuración del sistema remoto (si la comunidad predeterminada permite tales modificaciones)
Solución	Deshabilite el servicio SNMP en el host remoto si no lo usa. Filtre los paquetes UDP entrantes que van a este puerto o cambie la cadena de comunidad predeterminada.
Código Aplicaciones Afectadas	APP157

Vulnerabilidad	Unsupported Web Server Detection
Riesgo	Alto
Descripción	Según su versión, el servidor web está obsoleto y su proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.
Solución	Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.
Código Aplicaciones Afectadas	APP223, APP044, APP174

Tabla 2. Vulnerabilidades Altas sobre los servidores de aplicación del ambiente de certificación de los sistemas definidos para el 6to trimestre

4.1.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad	4.10.0 < 4.10.5 AC DC LDAP Server Denial of Service Vulnerability (CVE-2019-12436)
Riesgo	Medio
Descripción	La versión de Samba que se ejecuta en el host es la 4.10.0 anterior a la 4.10.5. Por lo tanto, está potencialmente afectado por una vulnerabilidad de denegación de servicio en el proceso del servidor LDAP de AD DC.
Solución	Actualice a Samba versión 4.10.5 o posterior.
Código Aplicaciones Afectadas	APP235

Vulnerabilidad	AgoraCart agora.cgi cart_id Parameter XSS
Riesgo	Medio
Descripción	Agora es un paquete de comercio electrónico basado en CGI. Debido a una validación de entrada deficiente, Agora permite que un atacante ejecute ataques de secuencias de comandos entre sitios.
Solución	Actualice a Agora 4.0e o más reciente.
Código Aplicaciones Afectadas	APP273

Vulnerabilidad (x6)	- Apache 2.4.x < 2.4.38 Multiple Vulnerabilities - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities - Apache >= 2.4.17 < 2.4.49 mod_http2 - Apache < 2.4.49 Multiple Vulnerabilities - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi
Riesgo	Medio
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache 2.4.49 o posterior.
Código Aplicaciones Afectadas	APP324, APP263

Vulnerabilidad	Apache Default Index Page
Riesgo	Medio
Descripción	El servidor web utiliza la página de índice de Apache predeterminada. Esta página puede contener algunos datos confidenciales como la raíz del servidor y las rutas de instalación.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP263

Vulnerabilidad	Apache HTTP Server httpOnly Cookie Information Disclosure
Riesgo	Medio

Descripción	La versión del servidor HTTP Apache que se ejecuta en el host se ve afectada por una vulnerabilidad de divulgación de información. Enviar una solicitud con encabezados HTTP lo suficientemente largos como para exceder el límite del servidor hace que el servidor web responda con un HTTP 400. De forma predeterminada, el encabezado y el valor HTTP ofensivos se muestran en la página de error 400. Cuando se usa junto con otros ataques (por ejemplo, secuencias de comandos entre sitios), esto puede resultar en el compromiso de las cookies httpOnly.
Solución	Actualice a Apache versión 2.0.65 / 2.2.22 o posterior.
Código Aplicaciones Afectadas	APP022, APP058

Vulnerabilidad	Apache mod_status /server-status Information Disclosure
Riesgo	Medio
Descripción	Un atacante remoto no autenticado puede obtener una descripción general de la actividad y el rendimiento del servidor web Apache remoto solicitando la URL '/estado-del-servidor'. Esta descripción general incluye información como los hosts actuales y las solicitudes que se procesan, la cantidad de trabajadores inactivos y solicitudes de servicio, y la utilización de la CPU.
Solución	Actualice los archivos de configuración de Apache para deshabilitar mod_status o restringir el acceso a hosts específicos.
Código Aplicaciones Afectadas	APP245, APP158, APP291, APP055, APP052, APP223, APP244

Vulnerabilidad	Apache ServerTokens Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web revelan información que puede ayudar a un atacante, como la versión del servidor, el sistema operativo y las versiones del módulo.
Solución	Cambie el valor de configuración de Apache ServerTokens a 'Prod'
Código Aplicaciones Afectadas	APP324, APP263

Vulnerabilidad (x25)	- Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK) - Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability - Apache Tomcat 7.0.0 < 7.0.104 Remote Code Execution - Apache Tomcat 7.0.x < 7.0.105 WebSocket DoS - Apache Tomcat 7.0.0 < 7.0.107 Information Disclosure - Apache Tomcat 7.0.0 < 7.0.108 RCE - Apache Tomcat 7.0.x < 7.0.53 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.54 XML Parser Information Disclosure - Apache Tomcat 7.0.x < 7.0.65 / 8.0.x < 8.0.27 Directory Traversal - Apache Tomcat < 7.0.67 Session Fixation - Apache Tomcat 7.0.x < 7.0.59 Security Manager Bypass - Apache Tomcat 7.0.x < 7.0.55 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.68 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control - Apache Tomcat 7.0.41 < 7.0.79 Cache Poisoning Vulnerability - Apache Tomcat 7.0.x < 7.0.82 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.81 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.88 Denial of Service - Apache Tomcat 7.0.0 < 7.0.85 Security Constraint Weakness

	- Apache Tomcat 7.0.0 < 7.0.91 Open Redirect Weakness - Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure - Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation - Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities - Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities - Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information DisclosurePHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error
Riesgo	Medio
Descripción	La versión de PHP instalada, se ve afectada por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a Apache Tomcat versión 7.0.109, 8.5.66, 9.0.46, 10.0.6 o posterior.
Código Aplicaciones Afectadas	APP223, APP044, APP174

Vulnerabilidad	Apache Tomcat Default Files
Riesgo	Medio
Descripción	La página de error predeterminada, la página de índice predeterminada, los JSP de ejemplo y/o los servlets de ejemplo son instalados en el servidor Apache Tomcat. Estos archivos deben eliminarse, ya que pueden ayudar a un atacante a descubrir información sobre la instalación de Tomcat o el propio host.
Solución	Elimine la página de índice predeterminada y elimine el JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error predeterminada.
Código Aplicaciones Afectadas	APP223, APP044, APP174

Vulnerabilidad	Apache Tomcat XSRF Token Disclosure
Riesgo	Medio
Descripción	El servidor web Apache Tomcat se ve afectado por una vulnerabilidad de divulgación de información en la página de índice de las aplicaciones Manager y Host Manager. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para obtener un token de falsificación de solicitud entre sitios (XSRF) válido durante la redirección emitida al solicitar /manager/ o /host-manager/. Este token puede ser utilizado por un atacante para construir un ataque XSRF.
Solución	Actualice a Apache Tomcat versión 7.0.68/8.0.32/9.0.0.M3 o posterior.
Código Aplicaciones Afectadas	APP223, APP044, APP174

Vulnerabilidad	Default nginx HTTP Server Settings
Riesgo	Medio
Descripción	El servidor web contiene configuraciones predeterminadas, como tokens de servidor habilitados y/o archivos predeterminados, como el índice predeterminado o las páginas de error. Estos elementos podrían potencialmente filtrar información útil sobre la instalación del servidor.
Solución	Deshabilite los tokens del servidor. Revise los archivos y reemplácelos o elimínelos según sea necesario.
Código Aplicaciones Afectadas	APP310

Vulnerabilidad	HTTP TRACE / TRACK Methods Allowed
Riesgo	Medio
Descripción	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Solución	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Código Aplicaciones Afectadas	APP324, APP263

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103, APP306, APP255, APP272, APP281, APP244, APP038, APP295

Vulnerabilidad	Linux Kernel TCP Sequence Number Generation Security Weakness
Riesgo	Medio
Descripción	El kernel de Linux es propenso a una debilidad de seguridad relacionada con la generación de números de secuencia TCP. Los atacantes pueden aprovechar este problema para inyectar paquetes arbitrarios en las sesiones TCP mediante un ataque de fuerza bruta. Un atacante puede usar esta vulnerabilidad para crear una condición de denegación de servicio o un ataque de intermediario.
Solución	Comuníquese con el proveedor del sistema operativo para obtener una actualización/parche del kernel de Linux.
Código Aplicaciones Afectadas	APP017, APP025

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web remoto utiliza la página de índice IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad (x2)	- nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE - nginx < 1.17.7 Information Disclosure
Riesgo	Medio
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.

Solución	Actualice a nginx 1.20.1 o posterior.
Código Aplicaciones Afectadas	APP310

Vulnerabilidad	Nonexistent Page (404) Physical Path Disclosure
Riesgo	Medio
Descripción	El servidor web revela la ruta física del webroot cuando se solicita una página inexistente. Si bien la impresión de errores en la salida es útil para depurar aplicaciones, esta función debe desactivarse en los servidores de producción.
Solución	Actualice el servidor web a la última versión. Como alternativa, vuelva a configurar el servidor web para deshabilitar los informes de depuración.
Código Aplicaciones Afectadas	APP253

Vulnerabilidad (x4)	- Oracle Database Multiple Vulnerabilities (January 2012 CPU) - Oracle Database Multiple Vulnerabilities (July 2012 CPU) - Oracle Database Multiple Vulnerabilities (October 2012 CPU) - Oracle Database Multiple Vulnerabilities (October 2013 CPU) (BEAST)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle.
Código Aplicaciones Afectadas	APP306

Vulnerabilidad	Oracle GlassFish Embedded Server Vulnerabilities (January 2016 CPU)
Riesgo	Medio
Descripción	La versión de Oracle GlassFish Server que se ejecuta en el host remoto se ve afectada por múltiples vulnerabilidades debido a fallas no especificadas relacionadas con el subcomponente Embedded Server. Un atacante remoto puede aprovecharlos para afectar la disponibilidad, la integridad y la confidencialidad. El vendedor no ha proporcionado más detalles.
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.14 o posterior, como se indica en el aviso de actualización de parches críticos de Oracle de enero de 2016.
Código Aplicaciones Afectadas	APP111

Vulnerabilidad (x3)	- Oracle GlassFish Server 3.1.2.x < 3.1.2.19 (October 2018 CPU) - Oracle GlassFish Server 3.0.1 / 3.1.2 / Enterprise 2.1.1 DoS - Oracle GlassFish Server 2.1.1.x < 2.1.1.29 / 3.0.1.x < 3.0.1.14 / 3.1.2.x < 3.1.2.15 Java Server Faces RCE (October 2016 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.19 o posterior, como se indica en el aviso de actualización de parche crítico de Oracle de octubre de 2018.
Código Aplicaciones Afectadas	APP111

Vulnerabilidad	Oracle GlassFish Server Multiple Vulnerabilities (October 2013 CPU)
Riesgo	Medio
Descripción	La versión de GlassFish Server que se ejecuta en el host remoto se ve afectada por múltiples vulnerabilidades en los siguientes componentes: - Caras del servidor Java - Metro
Solución	Actualice a GlassFish Server 2.1.1.22, 3.0.1.8, 3.1.2.7 o posterior.
Código Aplicaciones Afectadas	APP111

Vulnerabilidad	Oracle GlassFish Server Unspecified Information Disclosure (October 2015 CPU)
Riesgo	Medio
Descripción	La versión de Oracle GlassFish Server que se ejecuta en el host remoto se ve afectada por una vulnerabilidad de divulgación de información no especificada debido a una falla no especificada en el subcomponente de seguridad. Un atacante remoto puede explotar esto para revelar información confidencial.
Solución	Actualice a Oracle GlassFish Server 3.0.1.13, 3.1.2.13 o posterior como se indica en el aviso de actualización de parche crítico de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	

Descripción	Según su versión, la instalación de MySQL ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de MySQL que sea soportada actualmente.
Código Aplicaciones Afectadas	APP108

Vulnerabilidad	Oracle Database Multiple Vulnerabilities (October 2015 CPU)
Riesgo	Crítico
Descripción	Al servidor de base de datos de Oracle remoto le falta la Actualización de revisión crítica (CPU) de octubre de 2015. Por lo tanto, se ve afectado por múltiples vulnerabilidades en los siguientes componentes: - RDBMS básico (CVE-2015-4857) - Programador de base de datos (CVE-2015-4873) - Java VM (CVE-2015-4794, CVE-2015-4796, CVE-2015-4888) - Clusterware portátil (CVE-2015-4863) - Base de datos XDB-XML (CVE-2015-4900)
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	APP010, APP012, APP014, APP015, APP017, APP018, APP022, APP023 APP025, APP032, APP033, APP034, APP038, APP044, APP054, APP055, APP058, APP104, APP108, APP111, APP113, APP114, APP125, APP155, APP174, APP183, APP214, APP227, APP233, APP234, APP235, APP237, APP244, APP246, APP254, APP258, APP262, APP269, APP274, APP295, APP323

Vulnerabilidad	Oracle Database Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de Oracle Database que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle Database que sea compatible actualmente.
Código Aplicaciones Afectadas	APP023

Vulnerabilidad	Security Updates for Microsoft SQL Server 2016 and 2017 x64 (August 2018) (uncredentialed check)
Riesgo	Crítico
Descripción	Al servidor Microsoft SQL le falta una actualización de seguridad. Por lo tanto, se ve afectado por la vulnerabilidad de desbordamiento de búfer que permitiría la ejecución remota de código en un sistema afectado. Un atacante que aproveche con éxito la vulnerabilidad podría ejecutar código en el contexto de la cuenta de servicio del motor de base de datos de SQL Server.
Solución	Microsoft ha lanzado un conjunto de parches para las versiones x64 de SQL Server 2016 y 2017.
Código Aplicaciones Afectadas	APP260, APP039, APP071, APP230, APP236, APP283

Tabla 5. Vulnerabilidades Críticas sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre.

4.2.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.
Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP257

Vulnerabilidad	MS15-058: Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718) (uncredentialed check)
Riesgo	Alto
Descripción	La instalación remota de Microsoft SQL Server se ve afectada por múltiples vulnerabilidades: - Existe una vulnerabilidad de escalada de privilegios debido a la conversión de punteros a una clase incorrecta. Un atacante remoto autenticado puede explotar esto, a través de una consulta SQL especialmente diseñada, para obtener privilegios elevados. (CVE-2015-1761) - Existe una vulnerabilidad de ejecución remota de código debido al manejo incorrecto de llamadas de funciones internas a la memoria no inicializada. Un atacante puede explotar esto, a través de una consulta SQL especialmente diseñada en un servidor SQL afectado que tiene activada una configuración de permisos especiales (como VER ESTADO DEL SERVIDOR), para ejecutar código arbitrario. (CVE-2015-1762) - Existe una vulnerabilidad de ejecución remota de código debido al manejo incorrecto de llamadas de funciones internas a la memoria no inicializada. Un atacante remoto autenticado puede explotar esto, a través de una consulta SQL especialmente diseñada para ejecutar una función virtual desde una dirección incorrecta, para ejecutar código arbitrario. (CVE-2015-1762)
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2008, 2008 R2, 2012 y 2014.
Código Aplicaciones Afectadas	APP157

Vulnerabilidad (x7)	- MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows - MySQL < 5.0.83 Denial of Service - MySQL 5.7.x < 5.7.29 Multiple Vulnerabilities (Jan 2020 CPU) - MySQL 5.7.x < 5.7.24 Multiple Vulnerabilities (Oct 2018 CPU) (Jul 2019 CPU) - MySQL 5.7.x < 5.7.27 Multiple Vulnerabilities (Jul 2019 CPU) - MySQL 5.7.x < 5.7.21 Multiple Vulnerabilities (January 2018 CPU) - MySQL 5.7.x < 5.7.20 Multiple Vulnerabilities (October 2017 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.7.29 o posterior.

Código Aplicaciones Afectadas	APP108, APP008, APP087, APP088, APP089

Vulnerabilidad (x10)	- Oracle Database Multiple Vulnerabilities (April 2014 CPU) - Oracle Database Multiple Vulnerabilities (April 2015 CPU) - Oracle Database Multiple Vulnerabilities (April 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2015 CPU) - Oracle Database Multiple Vulnerabilities (January 2016 CPU) - Oracle Database Multiple Vulnerabilities (July 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2014 CPU) - Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK) - Oracle Database Multiple Vulnerabilities (October 2014 CPU) - Oracle Database Multiple Vulnerabilities (October 2017 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP010, APP012, APP014, APP015, APP017, APP018, APP022, APP023, APP025, APP032, APP033, APP034, APP038, APP044, APP054, APP055, APP058, APP104, APP108, APP111, APP113, APP114, APP125, APP155, APP174, APP183, APP214, APP227, APP233, APP234, APP235, APP237, APP244, APP246, APP254, APP258, APP262, APP269, APP274, APP295, APP323

Vulnerabilidad	SNMP Agent Default Community Name (public)
Riesgo	Alto
Descripción	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP remoto. Un atacante puede usar esta información para obtener más conocimiento sobre el host remoto o para cambiar la configuración del sistema remoto (si la comunidad predeterminada permite tales modificaciones)
Solución	Deshabilite el servicio SNMP en el host remoto si no lo usa. Filtre los paquetes UDP entrantes que van a este puerto o cambie la cadena de comunidad predeterminada.
Código Aplicaciones Afectadas	APP264

Tabla 6. Vulnerabilidades Altas sobre IP servidores de bases de datos de certificación de los sistemas definidos para el 6to trimestre.

4.2.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad	Apache mod_status /server-status Information Disclosure
Riesgo	Medio
Descripción	Un atacante remoto no autenticado puede obtener una descripción general de la actividad y el rendimiento del servidor web Apache remoto solicitando la URL '/estado-del-servidor'. Esta descripción general incluye información como los hosts actuales y las solicitudes que se procesan, la cantidad de trabajadores inactivos y solicitudes de servicio, y la utilización de la CPU.
Solución	Actualice los archivos de configuración de Apache para deshabilitar mod_status o restringir el acceso a hosts específicos.
Código Aplicaciones Afectadas	APP245, APP052

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103

Vulnerabilidad	KB4036996: Security Update for SQL Server (August 2017) (uncredentialed check)
Riesgo	Medio
Descripción	Al Microsoft SQL Server remoto le falta una actualización de seguridad. Por lo tanto, se ve afectado por una vulnerabilidad de divulgación de información en Microsoft SQL Server Analysis Services cuando aplica permisos de manera incorrecta. Un atacante podría aprovechar la vulnerabilidad si las credenciales del atacante permiten el acceso a una base de datos del servidor SQL afectada. Un atacante que aprovechara con éxito la vulnerabilidad puede obtener información adicional sobre la base de datos y los archivos.
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2012, 2014 y 2016.
Código Aplicaciones Afectadas	APP260, APP039, APP071, APP230, APP236, APP283

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web remoto utiliza la página de índice IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP039, APP071, APP230, APP236, APP283

Vulnerabilidad	MS16-136: Security Update for SQL Server (3199641) (uncredentialed check)
Riesgo	Medio
Descripción	Al Microsoft SQL Server remoto le falta una actualización de seguridad. Está, por tanto, afectado por múltiples vulnerabilidades: - Existen múltiples vulnerabilidades de elevación de privilegios en el motor SQL RDBMS debido al manejo inadecuado de la conversión de punteros. Un atacante remoto autenticado puede aprovecharlos para obtener privilegios elevados. (CVE-2016-7249, CVE-2016-7250, CVE-2016-7254) - Existe una vulnerabilidad de secuencias de comandos entre sitios (XSS) en la API de MDS del servidor SQL debido a una validación incorrecta de un parámetro de solicitud en el sitio del servidor SQL. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud especialmente diseñada, para ejecutar código arbitrario en la sesión del navegador del usuario. (CVE-2016-7251) - Existe una vulnerabilidad de divulgación de información en Microsoft SQL Analysis Services debido a una validación incorrecta de la ruta de FILESTREAM. Un atacante remoto autenticado puede explotar esto para revelar información confidencial de archivos y bases de datos. (CVE-2016-7252)

	- Existe una vulnerabilidad de elevación de privilegios en Microsoft SQL Server Engine debido a una verificación incorrecta por parte del Agente SQL Server de las ACL en atxcore.dll. Un atacante remoto autenticado puede explotar esto para obtener privilegios elevados. (CVE-2016-7253)
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2012, 2014 y 2016.
Código Aplicaciones Afectadas	APP157

Vulnerabilidad (x13)	- MySQL < 5.0.92 Multiple Denial of Service - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities - MySQL Denial of Service (Jul 2020 CPU) - MySQL 5.0 < 5.0.88 Multiple Vulnerabilities - MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass - MySQL 5.7.x < 5.7.22 Multiple Vulnerabilities (April 2018 CPU) - MySQL 5.7.x < 5.7.23 Multiple Vulnerabilities (July 2018 CPU) - MySQL 5.7.x < 5.7.25 Multiple Vulnerabilities (Jan 2019 CPU) - MySQL 5.7.x < 5.7.26 Multiple Vulnerabilities (Apr 2019 CPU) (Jul 2019 CPU) - MySQL 5.7.x < 5.7.28 Multiple Vulnerabilities (Oct 2019 CPU) - MySQL 5.7.x < 5.7.30 Multiple Vulnerabilities (Jan 2020 CPU) - MySQL 5.7.x < 5.7.31 Multiple Vulnerabilities (Jul 2020 CPU) - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a MySQL versión 5.0.88, 5.1.42, 5.5.0, 6.0.14 o posterior
Código Aplicaciones Afectadas	APP108, APP008, APP087, APP088, APP089

Vulnerabilidad	MySQL Binary Log SQL Injection
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host es anterior a 5.5.33 / 5.6.x anterior a 5.6.13 y, por lo tanto, está potencialmente afectada por múltiples vulnerabilidades de inyección de SQL. Los identificadores proporcionados por el usuario no se citan correctamente antes de escribirse en el registro binario. Un atacante con una cuenta válida y privilegios para modificar puede modificar tablas a las que no debería tener acceso.
Solución	Actualice a MySQL versión 5.5.33 / 5.6.13 o posterior.
Código Aplicaciones Afectadas	APP108

Vulnerabilidad (x8)	- Oracle Database Multiple Vulnerabilities (January 2018 CPU) - Oracle Database Server CVE-2018-3110 - Oracle Database Multiple Vulnerabilities (October 2016 CPU) - Oracle Database Multiple Vulnerabilities (April 2017 CPU) - Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU) - Oracle Database Multiple Vulnerabilities (January 2017 CPU) - Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32) - Oracle Database Multiple Vulnerabilities (January 2014 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades en varios de sus componentes.

Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP010, APP012, APP014, APP015, APP017, APP018, APP022, APP023, APP025, APP032, APP033, APP034, APP038, APP044, APP054, APP055, APP058, APP104, APP108, APP111, APP113, APP114, APP125, APP155, APP174, APP183, APP214, APP227, APP233, APP234, APP235, APP237, APP244, APP246, APP258, APP262, APP269, APP274, APP295, APP323

Vulnerabilidad	Security Updates for Microsoft SQL Server (Uncredentialed Check) (February 2020)
Riesgo	Medio
Descripción	A la instalación de Microsoft SQL Server en el host le falta una actualización de seguridad. Por tanto, se ve afectado por la siguiente vulnerabilidad: - Existe una vulnerabilidad de ejecución remota de código en Microsoft SQL Server Reporting Services cuando maneja incorrectamente las solicitudes de página. Un atacante que aproveche con éxito esta vulnerabilidad podría ejecutar código en el contexto de la cuenta de servicio del servidor de informes. (CVE-2020-0618)
Solución	Microsoft ha publicado las siguientes actualizaciones de seguridad para solucionar este problema: -KB4532095 -KB4532097 -KB4532098 -KB4535288 -KB4535706
Código Aplicaciones Afectadas	APP039, APP071, APP230, APP236, APP283, APP041

Vulnerabilidad	SNMP 'GETBULK' Reflection DDoS
Riesgo	Medio
Descripción	El demonio SNMP remoto está respondiendo con una gran cantidad de datos a una solicitud 'GETBULK' con un valor mayor que el normal para 'max-repetitions'. Un atacante remoto puede utilizar este servidor SNMP para realizar un ataque de denegación de servicio distribuido reflejado en un host remoto arbitrario.
Solución	Deshabilite el servicio SNMP en el host remoto si no lo usa. De lo contrario, restrinja y supervise el acceso a este servicio y considere cambiar la cadena de comunidad 'pública' predeterminada.
Código Aplicaciones Afectadas	APP264

Vulnerabilidad	SSH Weak Algorithms Supported
Riesgo	Medio
Descripción	Se ha detectado que el servidor SSH está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.
Código Aplicaciones Afectadas	APP264

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.

Código Aplicaciones Afectadas	APP260, APP023, APP041, APP290, APP307, APP157

Vulnerabilidad	SSL Certificate Expiry
Riesgo	Medio
Descripción	Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.
Solución	Compre o genere un nuevo certificado SSL para reemplazar el existente.
Código Aplicaciones Afectadas	APP023, APP290, APP307

Vulnerabilidad	SSL Certificate Signed Using Weak Hashing Algorithm
Riesgo	Medio
Descripción	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Solución	Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL.
Código Aplicaciones Afectadas	APP260, APP023, APP041, APP157

Vulnerabilidad	SSL Certificate with Wrong Hostname
Riesgo	Medio
Descripción	El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP260, APP267, APP041, APP157

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP260, APP023, APP041, APP157

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.

Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP008, APP023, APP047, APP087, APP088, APP089, APP157, APP257, APP260, APP267

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
Código Aplicaciones Afectadas	APP087, APP088, APP089, APP008, APP023, APP047, APP157, APP257, APP260, APP267

Tabla 7. Vulnerabilidades Medias sobre IP servidores de bases de datos de certificación de los sistemas definidos para el 6to trimestre.

4.2.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
Riesgo	Bajo
Descripción	La versión de MySQL instalada en el host remoto es anterior a 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 y, por lo tanto, no codifica correctamente los corchetes angulares cuando se usa la opción 'mysql --html'. Dependiendo de cómo se procese la salida del comando del cliente mysql, el usuario puede ser vulnerable a ataques de secuencias de comandos entre sitios.
Solución	Actualice a MySQL versión 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP108

Vulnerabilidad	SSH Server CBC Mode Ciphers Enabled
Riesgo	Bajo
Descripción	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado del modo de cifrado CBC y habilitar el cifrado del modo de cifrado CTR o GCM.
Código Aplicaciones Afectadas	APP264, APP243

Vulnerabilidad	SSH Weak MAC Algorithms Enabled
Riesgo	Bajo
Descripción	El servidor SSH remoto está configurado para permitir algoritmos MD5 o MAC de 96 bits, los cuales se consideran débiles.
Solución	Comuníquese con el proveedor o consulte la documentación del producto para deshabilitar los algoritmos MD5 y MAC de 96 bits.

Código Aplicaciones Afectadas	APP264

Vulnerabilidad	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Riesgo	Bajo
Descripción	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave de menos de 2048 bits. De acuerdo con los estándares de la industria establecidos por el foro de la autoridad de certificación/navegador (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048 bits. Algunas implementaciones SSL de navegador pueden rechazar claves de menos de 2048 bits después del 1 de enero de 2014. Además, algunos proveedores de certificados SSL pueden revocar certificados de menos de 2048 bits antes del 1 de enero de 2014
Solución	Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga y vuelva a emitir cualquier certificado firmado por el certificado anterior.
Código Aplicaciones Afectadas	APP041, APP157

Tabla 8. Vulnerabilidades Bajas sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre.

4.3 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN PRODUCCIÓN CON EXCEPCIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “F” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_6.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Producción-App” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas de acuerdo con la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja.

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.3.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad (x5)	- HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam) - HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593) - HP System Management Homepage < 7.1.1 Multiple Vulnerabilities - HP System Management Homepage < 6.3 Multiple Vulnerabilities - HP System Management Homepage < 7.0 Multiple Vulnerabilities
Riesgo	Crítico
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a HP System Management Homepage 7.5.4 o posterior.

Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico
Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.
Código Aplicaciones Afectadas	APP002, APP055, APP080, APP105, APP114, APP157, APP162, APP235, APP241, APP255, APP281

Vulnerabilidad	Microsoft IIS 6.0 Unsupported Version Detection
Riesgo	Crítico
Descripción	Según el número de la versión, la instalación de Microsoft Internet Information Services (IIS) 6.0 en el host ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Microsoft IIS que sea soportada actualmente.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Microsoft SQL Server Unsupported Version Detection (remote check)
Riesgo	Crítico
Descripción	Según su número de versión, ya no se admite la instalación de Microsoft SQL Server en el host remoto. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Microsoft SQL Server que sea compatible actualmente.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	MySQL 5.5.x < 5.5.53 Multiple Vulnerabilities (October 2016 CPU)
Riesgo	Crítico
Descripción	La versión de MySQL que se ejecuta en el host es 5.5.x anterior a 5.5.53. Por lo tanto, se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.5.53 o posterior.
Código Aplicaciones Afectadas	APP105

Vulnerabilidad	MySQL Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de MySQL ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución	Actualice a una versión de MySQL que sea soportada actualmente.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147

Vulnerabilidad (x7)	- Oracle Database Multiple Vulnerabilities (April 2007 CPU) - Oracle Database Multiple Vulnerabilities (April 2006 CPU) - Oracle Database Multiple Vulnerabilities (October 2009 CPU) - Oracle Database Multiple Vulnerabilities (January 2010 CPU) - Oracle Database Multiple Vulnerabilities (January 2006 CPU) - Oracle Database Multiple Vulnerabilities (July 2006 CPU) - Oracle Database Multiple Vulnerabilities (October 2015 CPU)
Riesgo	Crítico
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente a la vulnerabilidad reportada.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP266

Vulnerabilidad	Oracle Database Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de Oracle Database que se ejecuta en el host ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle Database que sea compatible actualmente.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)
Riesgo	Crítico
Descripción	El Oracle WebLogic Server remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS Core en la función readObject() debido a una desinfección incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de una carga útil de objeto manipulado, para eludir la lista negra ClassFilter.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2016.
Código Aplicaciones Afectadas	APP054, APP015, APP018

Vulnerabilidad	PHP Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión, la instalación de PHP en el host ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de PHP que sea soportada actualmente.

Código Aplicaciones Afectadas	APP151, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP324

Vulnerabilidad	SSL Version 2 and 3 Protocol Detection
Riesgo	Crítico
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. Un atacante puede aprovechar estas fallas para realizar ataques de man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo. NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía sólida" de PCI SSC.
Solución	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrado aprobados) o superior.
Código Aplicaciones Afectadas	APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP297, APP298

Vulnerabilidad	Unsupported Windows OS (remote)
Riesgo	Crítico
Descripción	El sistema operativo remoto o el paquete de servicio ya no son compatibles.
Solución	Actualice a un paquete de servicio o sistema operativo compatible.
Código Aplicaciones Afectadas	APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Tabla 9. Vulnerabilidades Críticas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre.

4.3.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad (x6)	- Apache 2.4.x < 2.4.39 Multiple Vulnerabilities - Apache 2.4.x < 2.4.47 Multiple Vulnerabilities - Apache < 2.4.49 Multiple Vulnerabilities - Apache 2.4.x < 2.4.46 Multiple Vulnerabilities - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities - Apache 2.4.x < 2.4.52 Multiple Vulnerabilities
Riesgo	Alto
Descripción	Según su banner, la versión de Apache que se ejecuta en el host remoto se ve afectado por varias vulnerabilidades.

Solución	Actualice a Apache versión 2.2.33, 2.4.53 o posterior.
Código Aplicaciones Afectadas	APP328, APP263, APP324

Vulnerabilidad	Apache HTTP Server Byte Range DoS
Riesgo	Alto
Descripción	La versión de Apache HTTP Server que se ejecuta en el host se ve afectada por una vulnerabilidad de denegación de servicio. Hacer una serie de solicitudes HTTP con rangos superpuestos en los encabezados de solicitud Range o Request-Range puede resultar en el agotamiento de la memoria y la CPU. Un atacante remoto no autenticado podría aprovechar esto para que el sistema no responda. El código de explotación está disponible públicamente.
Solución	Actualice a Apache httpd 2.2.21 o posterior. Alternativamente, aplique una de las soluciones en los avisos de Apache para CVE-2011-3192. La versión 2.2.20 solucionó el problema, pero también introdujo una regresión. Si el host ejecuta un servidor web basado en Apache httpd, comuníquese con el proveedor para obtener una solución.
Código Aplicaciones Afectadas	APP002, APP080

Vulnerabilidad (x9)	- Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities - Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilites - Apache Tomcat 8.5.0 < 8.5.40 Remote Code Execution Vulnerability (Windows) - Apache Tomcat 8.5.x < 8.5.13 / 9.0.x < 9.0.0.M19 Multiple Vulnerabilities - Apache Tomcat 8.5.0 < 8.5.32 Multiple Vulnerabilities - Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE) - Apache Tomcat 7.0.41 < 7.0.90 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
Riesgo	Alto
Descripción	El servidor Apache Tomcat se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache Tomcat versión 7.0.100, 8.5.51, 9.0.31 o posterior.
Código Aplicaciones Afectadas	APP032, APP214, APP296, APP297, APP298

Vulnerabilidad	Apache Tomcat AJP Connector Request Injection (Ghostcat)
Riesgo	Alto
Descripción	Se encontró una vulnerabilidad de lectura/inclusión de archivos en el conector AJP. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para leer archivos de aplicaciones web desde un servidor vulnerable. En los casos en que el servidor vulnerable permite la carga de archivos, un atacante podría cargar código malicioso de JavaServer Pages (JSP) dentro de una variedad de tipos de archivos y obtener la ejecución remota de código (RCE).
Solución	Actualice la configuración de AJP para requerir autorización y / o actualice el servidor Tomcat a 7.0.100, 8.5.51, 9.0.31 o posterior.
Código Aplicaciones Afectadas	APP008, APP087, APP088, APP089, APP241, APP300

Vulnerabilidad	Firewall UDP Packet Source Port 53 Ruleset Bypass

Riesgo	Alto
Descripción	Es posible eludir las reglas del firewall remoto enviando paquetes UDP con un puerto de origen igual a 53. Un atacante puede usar esta falla para inyectar paquetes UDP a los hosts remotos, a pesar de la presencia de un firewall.
Solución	Póngase en contacto con el proveedor para obtener una actualización o revise la configuración de las reglas del cortafuegos.
Código Aplicaciones Afectadas	APP234, APP244, APP258, APP251, APP014

Vulnerabilidad (x5)	- HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy) - HP System Management Homepage < 6.2 Multiple Vulnerabilities - HP System Management Homepage < 7.2.6 Multiple Vulnerabilities (FREAK) - HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities (BEAST) - HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution
Riesgo	Alto
Descripción	Según el banner del servidor web, la versión de HP System Management Homepage (SMH) alojada en el servidor web puede verse afectada por múltiples vulnerabilidades.
Solución	Actualice a HP System Management Homepage 7.6.1 o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	HP System Management Homepage ginkgosnmp.inc Command Injection
Riesgo	Alto
Descripción	Según el banner del servidor web, la versión de HP System Management Homepage (SMH) alojada en el servidor web remoto es anterior a la 7.2.2 y, por lo tanto, está afectada por una vulnerabilidad de inyección de comandos. Existe un error de validación de entrada en el archivo 'ginkgosnmp.inc' relacionado con el último segmento en una ruta URL solicitada. Esta entrada se usa más tarde en una llamada 'exec' y permitiría que un atacante autenticado ejecute comandos arbitrarios.
Solución	Actualice a HP System Management Homepage 7.2.2 o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Java JMX Agent Insecure Configuration
Riesgo	Alto
Descripción	Un agente Java JMX que se ejecuta en el host remoto está configurado sin cliente SSL y autenticación de contraseña. Un atacante remoto no autenticado puede conectarse al agente JMX y monitorear y administrar la aplicación Java que ha habilitado el agente. Además, esta configuración insegura permitiría al atacante crear un MBean javax.management.loading.MLet y usarlo para crear nuevos MBeans a partir de URL arbitrarias, al menos si no hay un administrador de seguridad. En otras palabras, el atacante podría ejecutar código arbitrario en el host remoto bajo el contexto de seguridad de la máquina virtual Java remota.
Solución	Habilite la autenticación de contraseña o cliente SSL para el agente JMX.
Código Aplicaciones Afectadas	APP297, APP298

Vulnerabilidad	ManageEngine ADManager Plus < Build 7115 RCE
Riesgo	Alto
Descripción	Zoho ManageEngine ADManager Plus anterior a la versión 7.1 Build 7115 se ve afectado por una falla de omisión de filtro que permite que un atacante remoto no autenticado cargue un archivo para ejecutar código arbitrario.
Solución	Actualice a ManageEngine ADManager Plus versión 7.1 compilación 7115 o posterior.
Código Aplicaciones Afectadas	APP041

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.
Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP257, APP269

Vulnerabilidad	Microsoft Windows SMB NULL Session Authentication
Riesgo	Alto
Descripción	El host está ejecutando Microsoft Windows. Es posible iniciar sesión usando una sesión NULL (es decir, sin nombre de usuario o contraseña). Dependiendo de la configuración, es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.
Solución	Aplique los siguientes cambios de registro según los avisos de Technet a los que se hace referencia. Colocar: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1 Reinicie una vez que se completen los cambios en el registro.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Microsoft Windows SMB Shares Unprivileged Access
Riesgo	Alto
Descripción	El control remoto tiene uno o más recursos compartidos de Windows a los que se puede acceder a través de la red con las credenciales proporcionadas. Dependiendo de los derechos compartidos, puede permitir que un atacante lea/escriba datos confidenciales.
Solución	Para restringir el acceso en Windows, abra el Explorador, haga clic derecho en cada recurso compartido, vaya a la pestaña 'compartir' y haga clic en 'permisos'.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Microsoft Windows SMBv1 Multiple Vulnerabilities
Riesgo	Alto

Descripción	El host de Windows remoto tiene activado el Bloque de mensajes de servidor de Microsoft 1.0 (SMBv1). Por tanto, se ve afectado por múltiples vulnerabilidades: - Existen múltiples vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades a través de un paquete SMBv1 especialmente diseñado para revelar información confidencial. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276) - Existen múltiples vulnerabilidades de denegación de servicio en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades, a través de una solicitud SMB especialmente diseñada, para hacer que el sistema deje de responder. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280) - Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades a través de un paquete SMBv1 especialmente diseñado para ejecutar código arbitrario. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279) Dependiendo de la configuración de la política de seguridad del host, este complemento no siempre puede determinar correctamente si el host de Windows es vulnerable si el host está ejecutando una versión posterior de Windows (es decir, Windows 8.1, 10, 2012, 2012 R2 y 2016) específicamente con nombre de canalizaciones y Se permite el acceso a los recursos compartidos de forma remota y anónima. Tenable no recomienda esta configuración, y los hosts deben comprobarse localmente en busca de parches con uno de los siguientes complementos, según la versión de Windows: 100054, 100055, 100057, 100059, 100060 o 100061.
Solución	Aplique la actualización de seguridad correspondiente a su versión de Windows.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Riesgo	Alto
Descripción	El host de Windows se ve afectado por las siguientes vulnerabilidades: - Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades a través de un paquete especialmente diseñado para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits de Equation Group divulgados el 14 de abril de 2017 por un grupo conocido como Shadow Brokers. WannaCry/WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.
Solución	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

	Para sistemas operativos Windows no compatibles, p. Ej. Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 carece de funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede desactivar siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de red. Para SMB sobre la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad (x4)	- MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows - MySQL < 5.0.83 Denial of Service - MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU) - MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.5.62 o posterior.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147, APP105

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1l Vulnerability
Riesgo	Alto
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1l. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1l. - Para descifrar los datos cifrados de SM2, se espera que una aplicación llame a la función API EVP_PKEY_decrypt(). Normalmente, una aplicación llamará a esta función dos veces. La primera vez, al ingresar, el parámetro de salida puede ser NULL y, al salir, el parámetro de salida se completa con el tamaño de búfer necesario para contener el texto sin formato descifrado. Luego, la aplicación puede asignar un búfer de tamaño suficiente y volver a llamar a EVP_PKEY_decrypt(), pero esta vez pasando un valor no NULL para el parámetro de salida. Un error en la implementación del código de descifrado SM2 significa que el cálculo del tamaño del búfer necesario para contener el texto sin formato devuelto por la primera llamada a EVP_PKEY_decrypt() puede ser menor que el tamaño real requerido por la segunda llamada. Esto puede provocar un desbordamiento del búfer cuando la aplicación llama a EVP_PKEY_decrypt() por segunda vez con un búfer demasiado pequeño. Un atacante malintencionado que pueda presentar contenido SM2 para descifrarlo en una aplicación podría hacer que los datos elegidos por el atacante desborden el búfer hasta un máximo de 62 bytes alterando el contenido de otros datos retenidos después del búfer, posiblemente cambiando el comportamiento de la aplicación o causando que la aplicación chocar. La ubicación del búfer depende de la aplicación, pero normalmente se asigna en montón. Corregido en OpenSSL 1.1.1l (Afectado 1.1.1-1.1.1k). (CVE-2021-3711). - Las cadenas ASN.1 se representan internamente dentro de OpenSSL como una estructura ASN1_STRING que contiene un búfer que contiene los datos de la cadena y un campo que contiene la longitud del búfer. Esto contrasta con las cadenas C normales que se representan como un búfer para los datos de cadena que terminan con un byte NUL (0). Aunque no es un requisito estricto, las cadenas ASN.1 que se analizan usando las propias funciones d2i de OpenSSL (y otras funciones de análisis similares), así como cualquier cadena cuyo valor se haya establecido con la función ASN1_STRING_set(), además, terminará con NUL la matriz de bytes en el Estructura ASN1_STRING. Sin embargo, es posible que las aplicaciones construyan directamente estructuras ASN1_STRING válidas que no terminan en NUL la matriz de bytes configurando directamente los campos de datos y longitud en la matriz ASN1_STRING. Esto también puede suceder usando la función ASN1_STRING_set0(). Se ha encontrado que numerosas funciones de OpenSSL que imprimen datos ASN.1 asumen que la matriz de bytes ASN1_STRING

	terminará en NUL, aunque esto no está garantizado para cadenas que se construyeron directamente. Cuando una aplicación solicita que se imprima una estructura ASN.1 y esa estructura ASN.1 contiene ASN1_STRING que ha construido directamente la aplicación sin que NUL termine el campo de datos, entonces puede ocurrir una saturación del búfer de lectura. Lo mismo puede ocurrir durante el procesamiento de certificados de restricciones de nombre (por ejemplo, si la aplicación ha construido directamente un certificado en lugar de cargarlo a través de las funciones de análisis de OpenSSL, y el certificado contiene estructuras ASN1_STRING que no terminan en NUL). También puede ocurrir en las funciones X509_get1_email(), X509_REQ_get1_email() y X509_get1_ocsp(). Si un actor malicioso puede hacer que una aplicación construya directamente un ASN1_STRING y luego lo procese a través de una de las funciones OpenSSL afectadas, entonces este problema podría verse afectado. Esto podría provocar un bloqueo (lo que provocaría un ataque de denegación de servicio). También podría dar lugar a la divulgación de contenidos de la memoria privada (como claves privadas o texto sin formato confidencial). Corregido en OpenSSL 1.1.1l (Afectado 1.1.1-1.1.1k). Corregido en OpenSSL 1.0.2za (Afectado 1.0.2-1.0.2y). (CVE-2021-3712).
Solución	Actualice a OpenSSL versión 1.1.1l o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad (x21)	- Oracle Database Multiple Vulnerabilities (April 2015 CPU) - Oracle Database Multiple Vulnerabilities (April 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK) - Oracle Database Multiple Vulnerabilities (October 2014 CPU) - Oracle Database Multiple Vulnerabilities (October 2017 CPU) - Oracle Database Multiple Vulnerabilities (April 2008 CPU) - Oracle Database Multiple Vulnerabilities (April 2010 CPU) - Oracle Database Multiple Vulnerabilities (April 2009 CPU) - Oracle Database Multiple Vulnerabilities (April 2011 CPU) - Oracle Database Multiple Vulnerabilities (January 2007 CPU) - Oracle Database Multiple Vulnerabilities (July 2007 CPU) - Oracle Database Multiple Vulnerabilities (July 2009 CPU) - Oracle Database Multiple Vulnerabilities (July 2011 CPU) - Oracle Database Multiple Vulnerabilities (July 2010 CPU) - Oracle Database Multiple Vulnerabilities (October 2007 CPU) - Oracle Database Multiple Vulnerabilities (October 2006 CPU) - Oracle Database Multiple Vulnerabilities (October 2011 CPU) - Oracle Database Multiple Vulnerabilities (October 2010 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente a la vulnerabilidad reportada.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP266

Vulnerabilidad (x8)	- Oracle Database Server Multiple Vulnerabilities (Apr 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Apr 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (July 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Oct 2019 CPU)

	- Oracle Database Server Multiple Vulnerabilities (October 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Jan 2020 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente a la vulnerabilidad reportada.
Código Aplicaciones Afectadas	APP266

Vulnerabilidad	Oracle WebLogic Java Object Deserialization RCE
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a llamadas de deserializado no seguras de objetos Java no autenticados a la biblioteca Apache Commons Collections (ACC). Un atacante remoto no autenticado puede explotar esto para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Actualice a la versión corregida relevante a la que se hace referencia en el aviso del proveedor.
Código Aplicaciones Afectadas	APP054, APP015, APP018

Vulnerabilidad	Oracle WebLogic Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de enero de 2017.
Código Aplicaciones Afectadas	APP054, APP015, APP018

Vulnerabilidad	Oracle WebLogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.3 Java Object Deserialization RCE (CVE-2018-3191)
Riesgo	Alto
Descripción	La versión de Oracle WebLogic Server instalada en el host remoto se ve afectada por una vulnerabilidad de ejecución remota de código en el subcomponente WLS Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java serializado diseñado, para ejecutar código arbitrario.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2018.
Código Aplicaciones Afectadas	APP125, APP054, APP104, APP155, APP233, APP227, APP246, APP114, APP234

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización no segura de objetos Java por parte del registro

	RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018
Código Aplicaciones Afectadas	APP054, APP233, APP114, APP234, APP015, APP018

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a una deserialización no segura de objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2018.
Código Aplicaciones Afectadas	APP054, APP233, APP114, APP234, APP015, APP018

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2019-2729)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en los paquetes wls9_async_response.war y wls-wsat.war debido a la deserialización no segura de objetos Java. Un atacante remoto no autenticado puede explotar el problema enviando un objeto serializado Java personalizado a través de una solicitud HTTP para ejecutar código Java arbitrario en el contexto del servidor web.
Solución	Aplique el parche adecuado de acuerdo con el aviso de alerta de seguridad de Oracle - CVE-2019-2729.
Código Aplicaciones Afectadas	APP015, APP018

Vulnerabilidad (x2)	- Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU) - Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2016.
Código Aplicaciones Afectadas	APP054, APP015, APP018

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (CVE-2018-3245)
Riesgo	Alto
Descripción	La versión de Oracle WebLogic Server instalada en el host remoto se ve afectada por una vulnerabilidad de ejecución remota de código en el subcomponente WLS Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java serializado diseñado, para ejecutar código arbitrario.
Solución	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2018 o actualice a una versión compatible para la que haya un parche disponible.

Código Aplicaciones Afectadas	APP125, APP054, APP104, APP155, APP233, APP227, APP246, APP114, APP234

Vulnerabilidad	Oracle WebLogic WLS9-async Remote Code Execution (remote check)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS9-async debido a la deserialización no segura de objetos Java codificados en XML. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche al que se hace referencia en el aviso del proveedor.
Código Aplicaciones Afectadas	APP054

Vulnerabilidad (x13)	- PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities - PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities - PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities - PHP < 4.4.8 Multiple Vulnerabilities - PHP < 4.4.5 Multiple Vulnerabilities - PHP < 4.4.7 / 5.2.2 Multiple Vulnerabilities - PHP < 4.4.9 Multiple Vulnerabilities - PHP < 4.4.4 Multiple Vulnerabilities - PHP < 5.2.11 Multiple Vulnerabilities - PHP < 5.2.8 Multiple Vulnerabilities - PHP < 5.3.9 Multiple Vulnerabilities - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution - PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabilities
Riesgo	Alto
Descripción	El servidor web remoto usa una versión de PHP que se ve afectada por múltiples fallas.
Solución	Actualice a la versión de PHP 5.3.12/5.4.2CGI o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Unsupported Web Server Detection
Riesgo	Alto
Descripción	Según su versión, el servidor web está obsoleto y su proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.
Solución	Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP122, APP032

Tabla 10. Vulnerabilidades Altas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre.

4.3.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad	AgoraCart agora.cgi cart_id Parameter XSS
Riesgo	Medio
Descripción	Agora es un paquete de comercio electrónico basado en CGI. Debido a una validación de entrada deficiente, Agora permite que un atacante ejecute ataques de secuencias de comandos entre sitios.
Solución	Actualice a Agora 4.0e o más reciente.
Código Aplicaciones Afectadas	APP273

Vulnerabilidad (x6)	- Apache 2.4.x < 2.4.38 Multiple Vulnerabilities - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities - Apache >= 2.4.17 < 2.4.49 mod_http2 - Apache < 2.4.49 Multiple Vulnerabilities - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi
Riesgo	Medio
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache 2.4.49 o posterior.
Código Aplicaciones Afectadas	APP328, APP263, APP324

Vulnerabilidad	Apache Default Index Page
Riesgo	Medio
Descripción	El servidor web utiliza la página de índice de Apache predeterminada. Esta página puede contener algunos datos confidenciales como la raíz del servidor y las rutas de instalación.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP162

Vulnerabilidad	Apache HTTP Server httpOnly Cookie Information Disclosure
Riesgo	Medio
Descripción	La versión de Apache HTTP Server que se ejecuta en el host remoto se ve afectada por una vulnerabilidad de divulgación de información. Enviar una solicitud con encabezados HTTP lo suficientemente largos como para exceder el límite del servidor hace que el servidor web responda con un HTTP 400. De forma predeterminada, el encabezado HTTP ofensivo y el valor se muestran en la página de error 400. Cuando se usa junto con otros ataques (p. ej., secuencias de comandos entre sitios), esto podría resultar en el compromiso de las cookies httpOnly.
Solución	Actualice a Apache versión 2.0.65 / 2.2.22 o posterior.
Código Aplicaciones Afectadas	APP002, APP022, APP080, APP152, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Apache ServerTokens Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor, el sistema operativo y las versiones del módulo.
Solución	Cambie el valor de configuración de Apache ServerTokens a 'Prod'
Código Aplicaciones Afectadas	APP328, APP263, APP324

Vulnerabilidad (x41)	- Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability - Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution - Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up - Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control - Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service - Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation - Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities - Apache Tomcat 8.5.x < 8.5.16 Multiple Vulnerabilities - Apache Tomcat 8.5.0 < 8.5.41 DoS - Apache Tomcat 8.5.x < 8.5.34 Open Redirect Weakness - Apache Tomcat 8.5.0 < 8.5.50 Privilege Escalation Vulnerability - Apache Tomcat 8.5.x < 8.5.55 Remote Code Execution - Apache Tomcat 8.5.0 < 8.5.49 Privilege Escalation - Apache Tomcat 8.5.0 < 8.5.57 Multiple Vulnerabilities - Apache Tomcat 8.5.0 < 8.5.63 Multiple Vulnerabilities - Apache Tomcat 8.5.0 < 8.5.56 DoS - Apache Tomcat 8.5.x < 8.5.60 Information Disclosure - Apache Tomcat 8.5.0 < 8.5.68 vulnerability - Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure - Apache Tomcat 8.5.x < 8.5.28 Security Constraint Weakness - Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK) - Apache Tomcat 7.0.0 < 7.0.104 Remote Code Execution - Apache Tomcat 7.0.0 < 7.0.107 Information Disclosure - Apache Tomcat 7.0.x < 7.0.105 WebSocket DoS - Apache Tomcat 7.0.0 < 7.0.108 RCE - Apache Tomcat 7.0.x < 7.0.53 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.55 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.59 Security Manager Bypass - Apache Tomcat 7.0.x < 7.0.65 / 8.0.x < 8.0.27 Directory Traversal - Apache Tomcat < 7.0.67 Session Fixation - Apache Tomcat 7.0.x < 7.0.68 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.54 XML Parser Information Disclosure - Apache Tomcat 7.0.x < 7.0.82 Multiple Vulnerabilities - Apache Tomcat 7.0.41 < 7.0.79 Cache Poisoning Vulnerability - Apache Tomcat 7.0.x < 7.0.81 Multiple Vulnerabilities - Apache Tomcat 7.0.0 < 7.0.85 Security Constraint Weakness - Apache Tomcat 7.0.x < 7.0.88 Denial of Service - Apache Tomcat 7.0.0 < 7.0.91 Open Redirect Weakness - Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure - Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities

	- Apache Tomcat 9.x < 9.0.40 Information Disclosure
Riesgo	Medio
Descripción	La versión de Apache Tomcat instalada en el host, se ve afectado por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a Apache Tomcat versión 7.0.109, 8.5.66, 9.0.46, 10.0.6 o posterior.
Código Aplicaciones Afectadas	APP214, APP297, APP298, APP032, APP301, APP296,

Vulnerabilidad (x8)	- Apache Tomcat 9.0.0.M1 < 9.0.16 DoS - Apache Tomcat 9.0.0.M1 < 9.0.12 Open Redirect Weakness - Apache Tomcat 9.0.0.M1 < 9.0.36 DoS - Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability - Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities - Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities - Apache Tomcat 9.0.0.M1 < 9.0.20 DoS - Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability
Riesgo	Medio
Descripción	La versión de Apache Tomcat instalada en el host, se ve afectado por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Upgrade to Apache Tomcat version 9.0.48 or later.
Código Aplicaciones Afectadas	APP214, APP301

Vulnerabilidad	Apache Tomcat Default Files
Riesgo	Medio
Descripción	La página de error predeterminada, la página de índice predeterminada, los JSP de ejemplo y/o los servlets de ejemplo se instalan en el servidor Apache Tomcat remoto. Estos archivos deben eliminarse, ya que pueden ayudar a un atacante a descubrir información sobre la instalación remota de Tomcat o el propio host.
Solución	Elimine la página de índice predeterminada y elimine el JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error predeterminada.
Código Aplicaciones Afectadas	APP214, APP297, APP298, APP301, APP296

Vulnerabilidad	Apache Tomcat XSRF Token Disclosure
Riesgo	Medio
Descripción	El servidor web Apache Tomcat remoto se ve afectado por una vulnerabilidad de divulgación de información en la página de índice de las aplicaciones Manager y Host Manager. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para obtener un token de falsificación de solicitud entre sitios (XSRF) válido durante la redirección emitida al solicitar /manager/ o /host-manager/. Este token puede ser utilizado por un atacante para construir un ataque XSRF.
Solución	Actualice a Apache Tomcat versión 7.0.68/8.0.32/9.0.0.M3 o posterior.
Código Aplicaciones Afectadas	APP032

Vulnerabilidad	Echo Service Detection

Riesgo	Medio
Descripción	El host remoto está ejecutando el servicio 'echo'. Este servicio se hace eco de los datos que se le envían. Este servicio no se utiliza en estos días, por lo que se desactivar, ya que los atacantes pueden utilizarlo para configurar ataques de denegación de servicios contra este host.
Solución	A continuación, se muestran algunos ejemplos de cómo deshabilitar el servicio de eco en algunas plataformas; sin embargo, muchos servicios pueden exhibir este comportamiento y la lista a continuación no es exhaustiva. Consulte la documentación del proveedor del servicio que muestra el comportamiento del eco para obtener más información. - En sistemas Unix, comente la línea 'echo' en /etc/inetd.conf y reinicie el proceso inetd. - En los sistemas Ubuntu, comente la línea 'echo' en /etc/systemd/system.conf y vuelva a iniciar el servicio systemd. - En los sistemas Windows, establezca la siguiente clave de registro en 0: HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEchoHKLM\System\ CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Luego inicie cmd.exe y escriba: net stop simptcp net start simptcp
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad (x4)	- HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities - HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753) - HP System Management Homepage < 7.3 Multiple Vulnerabilities - HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE)
Riesgo	Medio
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a HP System Management Homepage 7.6.1 o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	HSTS Missing From HTTPS Server (RFC 6797)
Riesgo	Medio
Descripción	El servidor web remoto no está aplicando HSTS, como se define en RFC 6797. HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicarle al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de man-in-the-middle, de eliminación de SSL y debilita las protecciones contra el secuestro de cookies.
Solución	Configure el servidor web remoto para usar HSTS.
Código Aplicaciones Afectadas	APP304

Vulnerabilidad	HTTP TRACE / TRACK Methods Allowed
Riesgo	Medio

Descripción	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Solución	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Código Aplicaciones Afectadas	APP328, APP022, APP263, APP324, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103, APP244, APP306, APP256, APP323, APP038, APP295, APP255

Vulnerabilidad	Linux Kernel TCP Sequence Number Generation Security Weakness
Riesgo	Medio
Descripción	El kernel de Linux es propenso a una debilidad de seguridad relacionada con la generación de números de secuencia TCP. Los atacantes pueden aprovechar este problema para inyectar paquetes arbitrarios en las sesiones TCP mediante un ataque de fuerza bruta. Un atacante puede usar esta vulnerabilidad para crear una condición de denegación de servicio o un ataque de intermediario. Tenga en cuenta que este complemento puede activarse como resultado de un dispositivo de red (como un equilibrador de carga, VPN, IPS, proxy transparente, etc.) que es vulnerable y que reescribe los números de secuencia de TCP, en lugar de que el propio host sea vulnerable.
Solución	Comuníquese con el proveedor del sistema operativo para obtener una actualización/parche del kernel de Linux.
Código Aplicaciones Afectadas	APP002, APP080, APP022, APP017, APP025

Vulnerabilidad (x3)	- MariaDB 10.3.0 < 10.3.22 A Vulnerability - MariaDB 10.3.0 < 10.3.23 Multiple Vulnerabilities - MariaDB 10.3.x < 10.3.19 Multiple Denial of Service Vulnerabilities
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MariaDB versión 10.3.23 o posterior.
Código Aplicaciones Afectadas	APP131

Vulnerabilidad	mDNS Detection (Remote Network)
Riesgo	Medio

Descripción	El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite que cualquier persona descubra información del host remoto, como su tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando. Este complemento intenta descubrir mDNS utilizados por hosts que no están en el segmento de red en el que reside Nessus.
Solución	Filtre el tráfico entrante al puerto UDP 5353, si lo desea.
Código Aplicaciones Afectadas	APP002, APP080

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web remoto utiliza la página de índice IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP297, APP298, APP296

Vulnerabilidad	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Riesgo	Medio
Descripción	La versión remota del servidor de protocolo de escritorio remoto (Terminal Service) es vulnerable a un ataque man-in-the-middle (MiTM). El cliente RDP no hace ningún esfuerzo por validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer un cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información confidencial transmitida, incluidas las credenciales de autenticación. Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y usarla para este ataque.
Solución	Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o seleccione la opción 'Permitir conexiones solo desde equipos que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
Riesgo	Medio
Descripción	Existe una vulnerabilidad de ejecución remota de código en la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja ciertas solicitudes. Un atacante que aproveche con éxito la vulnerabilidad podría obtener la capacidad de ejecutar código en el servidor de destino (CVE - 2017-11780). Existe una vulnerabilidad de denegación de servicio en el mensaje de bloqueo del servidor (SMB) de Microsoft cuando un atacante envía solicitudes especialmente diseñadas al servidor. Un atacante que aproveche esta vulnerabilidad podría hacer que el sistema afectado se bloquee. Para intentar aprovechar este problema, un atacante debería enviar solicitudes SMB especialmente diseñadas al sistema de destino. Tenga en cuenta que la vulnerabilidad de denegación de servicio no permitiría a un atacante ejecutar código o elevar sus derechos de usuario, pero podría hacer que el sistema afectado dejara de aceptar solicitudes. La actualización de seguridad

	corrige la vulnerabilidad al corregir la forma en que SMB maneja las solicitudes de clientes especialmente diseñadas (CVE - 2017-11781).
Solución	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	MS11-049: Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893) (uncredentialed check)
Riesgo	Medio
Descripción	Una aplicación en el host remoto tiene una vulnerabilidad de divulgación de información. Al analizar un archivo de detección de servicios web (.disco) especialmente diseñado, se permiten entidades XML externas para la entrada de usuarios que no son de confianza. Un atacante remoto podría explotar esto engañando a un usuario para que abra un archivo .disco especialmente diseñado, lo que resultaría en la divulgación de información confidencial.
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2005, 2008 y 2008 R2.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Riesgo	Medio
Descripción	El host de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación en los canales de Llamada a procedimiento remoto (RPC). Un atacante intermediario capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede aprovechar esto para forzar la degradación del nivel de autenticación, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM.
Solución	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad (x11)	- MySQL 5.0 < 5.0.88 Multiple Vulnerabilities - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities - MySQL < 5.0.92 Multiple Denial of Service - MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass - MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU) - MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU) - MySQL 5.5.x < 5.5.54 Multiple Vulnerabilities (January 2017 CPU) - MySQL 5.5.x < 5.5.55 Multiple Vulnerabilities (April 2017 CPU) (Riddle) - MySQL 5.5.x < 5.5.58 Multiple Vulnerabilities (October 2017 CPU) - MySQL 5.5.x < 5.5.57 Multiple Vulnerabilities (July 2017 CPU) - MySQL 5.1.x < 5.7.3 SSL/TLS Downgrade MitM (BACKRONYM)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.7.3 o posterior.

Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147, APP105

Vulnerabilidad	MySQL Binary Log SQL Injection
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host es anterior a 5.5.33 / 5.6.x anterior a 5.6.13 y, por lo tanto, está potencialmente afectada por múltiples vulnerabilidades de inyección de SQL. Los identificadores proporcionados por el usuario no se citan correctamente antes de escribirse en el registro binario. Un atacante con una cuenta válida y privilegios para modificar puede modificar tablas a las que no debería tener acceso.
Solución	Actualice a MySQL versión 5.5.33 / 5.6.13 o posterior.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147

Vulnerabilidad	MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de MySQL Community Server instalada en el host remoto es anterior a la 5.1.47 / 5.0.91 y, por lo tanto, está potencialmente afectada por las siguientes vulnerabilidades: - El servidor puede continuar leyendo paquetes indefinidamente si recibe un paquete mayor que el tamaño máximo de un paquete, lo que podría permitir que un atacante remoto no autenticado consuma un alto nivel de CPU y ancho de banda. (Error #50974) - Usando un argumento de nombre de tabla demasiado largo para el comando 'COM_FIELD_LIST', un usuario autenticado puede desbordar un búfer y ejecutar código arbitrario en el host afectado. (Error #53237) - Usando un argumento de nombre de tabla especialmente diseñado para 'COM_FIELD_LIST', un usuario autenticado puede omitir casi todas las formas de verificación de privilegios y concesiones a nivel de tabla. (Error #53371)
Solución	Actualice a MySQL Community Server 5.1.47 / 5.0.91 o posterior.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147

Vulnerabilidad	MySQL Denial of Service (Jul 2020 CPU)
Riesgo	Medio
Descripción	La versión de MySQL que se ejecuta en el host es menor a 5.7.29 o menor a 8.0.19. Por lo tanto, se ve afectado por una vulnerabilidad, como se indica en el aviso de actualización del parche crítico de julio de 2020: Una vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Servidor: Replicación). Las versiones compatibles que se ven afectadas son menores a 5.7.29 y menores a 8.0.19. La vulnerabilidad fácilmente explotable permite que un atacante con muchos privilegios con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server.
Solución	Consulte el aviso del proveedor.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147, APP105

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión del producto probado instalado en el host remoto es anterior a la versión probada
Solución	Actualice a OpenSSL versión 1.1.1d o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1e-dev. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1e-dev.
Solución	Actualice a OpenSSL versión 1.1.1e-dev o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability
Riesgo	Medio
Descripción	La versión del producto probado instalado en el host remoto es anterior a la versión probada. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1i.
Solución	Actualice a OpenSSL versión 1.1.1i o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1j Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1j. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 1.1.1j.
Solución	Actualice a OpenSSL versión 1.1.1jo posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1k Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1k. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 1.1.1k.
Solución	Actualice a OpenSSL versión 1.1.1k o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1m Vulnerability

Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1m. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1m.
Solución	Actualice a OpenSSL versión 1.1.1m o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1n Vulnerability
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1n. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1n.
Solución	Actualice a OpenSSL versión 1.1.1n o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad (x10)	- Oracle Database Multiple Vulnerabilities (April 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2018 CPU) - Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32) - Oracle Database Multiple Vulnerabilities (October 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2008 CPU) - Oracle Database Multiple Vulnerabilities (January 2012 CPU) - Oracle Database Multiple Vulnerabilities (January 2009 CPU) - Oracle Database Multiple Vulnerabilities (July 2008 CPU) - Oracle Database Multiple Vulnerabilities (October 2008 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente al anuncio de la vulnerabilidad.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP266

Vulnerabilidad (x2)	- Oracle Database Server CVE-2018-3110 - Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente al anuncio de la vulnerabilidad.
Código Aplicaciones Afectadas	APP266

Vulnerabilidad	Oracle Database Server Multiple Vulnerabilities (Jan 2019 CPU)
Riesgo	Medio
Descripción	Al servidor de base de datos Oracle remoto le falta la actualización de parche crítico (CPU) de enero de 2019.

Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de enero de 2019.
Código Aplicaciones Afectadas	APP266

Vulnerabilidad	Oracle WebLogic WSAT Remote Code Execution
Riesgo	Medio
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el extremo WSAT debido a la deserialización no segura de objetos Java codificados en XML. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2017.
Código Aplicaciones Afectadas	APP054

Vulnerabilidad (x15)	- PHP 7.4.x < 7.4.28 - PHP < 7.3.28 Email Header Injection - PHP < 7.3.24 Multiple Vulnerabilities - PHP 7.4.x < 7.4.25 - PHP 7.4.x < 7.4.26 - PHP 7.4.x < 7.4.18 / 8.x < 8.0.5 Integer Overflow - PHP 7.3.x < 7.3.25 / 7.4.x < 7.4.13 Multiple Vulnerabilities - PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error - PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS - PHP 7.4.x < 7.4.12 DoS - PHP < 5.2.10 Multiple Vulnerabilities - PHP < 5.2.12 Multiple Vulnerabilities - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities - PHP < 5.2.9 Multiple Vulnerabilities - PHP < 5.3.11 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de PHP instalada en el host, se ve afectada por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a la versión de PHP 7.3.28, 7.4.18, 8.0.5 o posterior.
Código Aplicaciones Afectadas	APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP327, APP151, APP158, APP175 APP255, APP281, APP285, APP287, APP292, APP324, APP329

Vulnerabilidad	PHP Multiple Image Processing Functions File Handling DoS
Riesgo	Medio
Descripción	Según su banner, la versión de PHP instalada en el host es vulnerable a un ataque de denegación de servicio debido a que no valida correctamente los datos del archivo en las rutinas 'php_handle_iff' y 'php_handle_jpeg', que son llamadas por la función PHP ' getimagesize '. Usando un archivo de imagen especialmente diseñado, un atacante puede desencadenar un bucle infinito cuando se llama a 'getimagesize', quizás incluso de forma remota en los casos en que se permite la carga de imágenes.
Solución	Actualice a PHP 4.3.11 / 5.0.4 o posterior.

Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SMB Signing not required
Riesgo	Medio
Descripción	No es requerida una firma en el servidor SMB. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de man-in-the-middle contra el servidor SMB.
Solución	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Consulte los enlaces "ver también" para obtener más detalles.
Código Aplicaciones Afectadas	APP304, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SSH Weak Algorithms Supported
Riesgo	Medio
Descripción	Se ha detectado que el servidor SSH está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.
Código Aplicaciones Afectadas	APP306, APP302

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloque con bloques de 64 bits en uno o más conjuntos de cifrado. Por lo tanto, se ve afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de cifrados de bloque débiles de 64 bits. Un atacante intermediario que tenga suficientes recursos puede explotar esta vulnerabilidad, a través de un ataque de 'birthday', para detectar una colisión que filtre el XOR entre el secreto fijo y un texto plano conocido, permitiendo la divulgación del texto secreto, como las cookies HTTPS seguras, y posiblemente resulte en el secuestro de una sesión autenticada.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloque de 64 bits. Alternativamente, establezca limitaciones en la cantidad de solicitudes que se pueden procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Código Aplicaciones Afectadas	APP055, APP223, APP297, APP298, APP122, APP318, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP032, APP035, APP038, APP044, APP055, APP057, APP058, APP107, APP122, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP245, APP253, APP255, APP256, APP265, APP304, APP306, APP318, APP328

Vulnerabilidad	SSL Certificate Expiry
Riesgo	Medio
Descripción	Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.
Solución	Compre o genere un nuevo certificado SSL para reemplazar el existente.
Código Aplicaciones Afectadas	APP256, APP245, APP253, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SSL Certificate Signed Using Weak Hashing Algorithm
Riesgo	Medio
Descripción	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Solución	Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL.
Código Aplicaciones Afectadas	APP032, APP035, APP038, APP044, APP057, APP058, APP107, APP122, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SSL Certificate with Wrong Hostname
Riesgo	Medio
Descripción	El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP039, APP297, APP298, APP041, APP122, APP277, APP296

Vulnerabilidad	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Riesgo	Medio
Descripción	El host remoto admite SSLv2 y, por lo tanto, puede verse afectado por una vulnerabilidad que permite un ataque de Oracle de relleno Bleichenbacher entre protocolos conocido como DROWN (Descifrado de RSA con cifrado obsoleto y debilitado). Esta vulnerabilidad existe debido a una falla en la implementación de Secure Sockets Layer Versión 2 (SSLv2), y permite descifrar el tráfico TLS capturado. Un atacante man-in-the-middle puede aprovechar esto para descifrar la conexión TLS utilizando tráfico capturado previamente y criptografía débil junto con una serie de conexiones especialmente diseñadas a un servidor SSLv2 que usa la misma clave privada.
Solución	Deshabilite SSLv2 y los conjuntos de cifrado de criptografía de grado de exportación. Asegúrese de que las claves privadas no se utilicen en ningún lugar con software de servidor que admita conexiones SSLv2.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	SSL Medium Strength Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Código Aplicaciones Afectadas	APP055, APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP223, APP265, APP297, APP298, APP318

Vulnerabilidad	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Riesgo	Medio
Descripción	El host admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en la generación de un flujo de bytes pseudoaleatorio, por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
Código Aplicaciones Afectadas	APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP297, APP298

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP328, APP032, APP035, APP038, APP044, APP055, APP057, APP058, APP107, APP122, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP255, APP265, APP304, APP306, APP318

Vulnerabilidad	SSL Weak Cipher Suites Supported
Riesgo	Medio
Descripción	El host remoto admite el uso de cifrados SSL que ofrecen un cifrado débil.
Solución	Reconfigure la aplicación afectada, si es posible para evitar el uso de cifrados débiles.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Riesgo	Medio
Descripción	El host se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados mediante cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC). Los atacantes MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas. Siempre que un cliente y un servicio sean compatibles con SSLv3, una conexión se puede "revertir" a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o una versión posterior. El mecanismo TLS Fallback SCSV evita los ataques de "reversión de versiones" sin afectar a los clientes heredados; sin embargo, solo puede proteger las conexiones cuando el cliente y el servicio admiten el mecanismo. Los sitios que no pueden deshabilitar SSLv3 de inmediato deben habilitar este mecanismo. Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación de SSL en particular. Desactivar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.

Solución	Desactive SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda inhabilitar SSLv3.
Código Aplicaciones Afectadas	APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP297, APP298

Vulnerabilidad	Terminal Services Encryption Level is Medium or Low
Riesgo	Medio
Descripción	El servicio de Terminal Services remoto no está configurado para utilizar criptografía sólida. El uso de criptografía débil con este servicio permite que un atacante espíe las comunicaciones más fácilmente y obtenga capturas de pantalla y/o pulsaciones de teclado.
Solución	Cambie el nivel de cifrado RDP a uno de los siguientes: 3. High 4. FIPS Compliant
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP087, APP088, APP089, APP119, APP120, APP121, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP295, APP298, APP003, APP008, APP010, APP021, APP030, APP038, APP039, APP041, APP055, APP071, APP073, APP074, APP108, APP122, APP156, APP175, APP214, APP233, APP241, APP256, APP277, APP296, APP297, APP300, APP301, APP304, APP306, APP318, APP322, APP323

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
Código Aplicaciones Afectadas	APP087, APP088, APP089, APP119, APP120, APP121, APP295, APP298, APP003, APP008, APP010, APP021, APP030, APP038, APP039, APP041, APP055, APP071, APP073, APP074, APP108, APP122, APP156, APP214, APP233, APP241, APP256, APP257, APP277, APP296, APP297, APP300, APP301, APP304, APP306, APP318, APP322, APP323

Vulnerabilidad	Web Server Error Page Information Disclosure
Riesgo	Medio
Descripción	La página de error predeterminada enviada por el servidor web remoto revela información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique el servidor web para no revelar información detallada sobre el servidor web subyacente o utilice una página de error personalizada en su lugar.
Código Aplicaciones Afectadas	APP032, APP044, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP296, APP297, APP298

Vulnerabilidad	Web Server Expect Header XSS
Riesgo	Medio
Descripción	El servidor web remoto no puede desinfectar el contenido de un encabezado de solicitud 'Expect' antes de usarlo para generar contenido web dinámico. Un atacante remoto no autenticado puede aprovechar este problema para lanzar ataques de secuencias de comandos entre sitios contra el servicio afectado, quizás a través de archivos ShockWave (SWF) especialmente diseñados.
Solución	Consulte con el proveedor para obtener una actualización del servidor web. Para Apache, el problema se ha solucionado según se informa en las versiones 1.3.35 / 2.0.57 / 2.2.2; para IBM HTTP Server, actualice a 6.0.2.13 / 6.1.0.1; para IBM WebSphere Application Server, actualice a 5.1.1.17
Código Aplicaciones Afectadas	APP022, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique los encabezados HTTP del servidor web para no revelar información detallada sobre el servidor web subyacente.
Código Aplicaciones Afectadas	APP022, APP041, APP122, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP256, APP263, APP265, APP296, APP297, APP298, APP324, APP328

Tabla 11. Vulnerabilidades Medias sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre.

4.3.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	HP System Management Homepage < 7.5.4.3 AddCertsToTrustCfgList DoS
Riesgo	Bajo
Descripción	La versión de HP System Management Homepage (SMH) alojada en el servidor web remoto es anterior a la 7.5.4.3. Por lo tanto, se ve afectado por una falla en la función AddCertsToTrustCfgList() dentro del archivo mod_smh_config.so debido a una extracción incorrecta del nombre común en el asunto al procesar certificados X.509. Un atacante remoto no autenticado puede aprovechar este problema, a través de un certificado elaborado, para provocar una condición de denegación de servicio. Tenga en cuenta que, para aprovechar esta vulnerabilidad, la configuración 'Modo de confianza' debe configurarse con 'Confiar en todos', la configuración 'Inicio de sesión restringido por IP' debe permitir que el atacante acceda a SMH y la configuración 'Autorización Kerberos' (solo Windows) debe estar deshabilitado.
Solución	Actualice a HP System Management Homepage (SMH) versión 7.5.4.3 o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
Riesgo	Bajo
Descripción	La versión de MySQL instalada en el host remoto es anterior a 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 y, por lo tanto, no codifica correctamente los corchetes angulares cuando se usa la opción 'mysql --html'. Dependiendo

	de cómo se procese la salida del comando del cliente mysql, el usuario puede ser vulnerable a ataques de secuencias de comandos entre sitios.
Solución	Actualice a MySQL versión 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP051, APP126, APP136, APP146, APP147

Vulnerabilidad	PHP < 4.4.2 Multiple XSS Vulnerabilities
Riesgo	Bajo
Descripción	Según su banner, la versión de PHP instalada en el host remoto es anterior a la 4.4.2. Dichas versiones se ven potencialmente afectadas por múltiples vulnerabilidades de secuencias de comandos entre sitios cuando están activados display_errors y html_errors.
Solución	Actualice a la versión de PHP 4.4.2 o posterior.
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Vulnerabilidad	SSH Server CBC Mode Ciphers Enabled
Riesgo	Bajo
Descripción	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado del modo de cifrado CBC y habilitar el cifrado del modo de cifrado CTR o GCM.
Código Aplicaciones Afectadas	APP306, APP302, APP049, APP303, APP151, APP152, APP154, APP338

Vulnerabilidad	SSL Anonymous Cipher Suites Supported
Riesgo	Bajo
Descripción	El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite a un administrador configurar un servicio que cifra el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de man-in-the-middle.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados débiles.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Riesgo	Bajo
Descripción	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave de menos de 2048 bits. De acuerdo con los estándares de la industria establecidos por el foro de la autoridad de certificación/navegador (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048 bits. Algunas implementaciones SSL de navegador pueden rechazar claves de menos de 2048 bits después del 1 de enero de 2014. Además, algunos proveedores de certificados SSL pueden revocar certificados de menos de 2048 bits antes del 1 de enero de 2014
Solución	Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga y vuelva a emitir cualquier certificado firmado por el certificado anterior.

Código Aplicaciones Afectadas	APP122

Vulnerabilidad	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Riesgo	Bajo
Descripción	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en un corto período de tiempo (según el tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.
Solución	Vuelva a configurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o más.
Código Aplicaciones Afectadas	APP055, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265, APP297, APP298, APP306

Vulnerabilidad	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Riesgo	Bajo
Descripción	El host admite conjuntos de cifrado EXPORT_DHE con claves menores o iguales a 512 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en poco tiempo. Un atacante man-in-the-middle puede degradar la sesión para usar conjuntos de cifrado EXPORT_DHE. Por lo tanto, se recomienda eliminar el soporte para conjuntos de cifrado débiles.
Solución	Vuelva a configurar el servicio para eliminar la compatibilidad con los conjuntos de cifrado EXPORT_DHE.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	Terminal Services Encryption Level is not FIPS-140 Compliant
Riesgo	Bajo
Descripción	La configuración de cifrado utilizada por el servicio de Terminal Services remoto no es compatible con FIPS-140.
Solución	Cambie el nivel de cifrado RDP a: 4. FIPS Compliant
Código Aplicaciones Afectadas	APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP265

Tabla 12. Vulnerabilidades Bajas sobre servidores de aplicación del ambiente de producción de los sistemas definidos para el 6to trimestre.

4.4 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDOR DE BASES DE DATOS - PRODUCCIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “G” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_6.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Producción-DB” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas de acuerdo con la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja.

Vulnerabilidad	Oracle Database Multiple Vulnerabilities (October 2015 CPU)
Riesgo	Crítico
Descripción	Al servidor de base de datos de Oracle remoto le falta la Actualización de revisión crítica (CPU) de octubre de 2015. Por lo tanto, se ve afectado por múltiples vulnerabilidades en los siguientes componentes: - RDBMS básico (CVE-2015-4857) - Programador de base de datos (CVE-2015-4873) - Java VM (CVE-2015-4794, CVE-2015-4796, CVE-2015-4888) - Clusterware portátil (CVE-2015-4863) - Base de datos XDB-XML (CVE-2015-4900)
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	APP002, APP005, APP010, APP012, APP014, APP015, APP017, APP018, APP019, APP022, APP023, APP025, APP026, APP032, APP033, APP034, APP035, APP038, APP044, APP054, APP055, APP058, APP058, APP080, APP084, APP104, APP108, APP110, APP111, APP113, APP114, APP123, APP125, APP155, APP173, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP214, APP227, APP233, APP234, APP235, APP237, APP241, APP244, APP246, APP254, APP258, APP262, APP265, APP266, APP295

Vulnerabilidad	PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Multiple Vulnerabilities
Riesgo	Crítico
Descripción	La versión de PostgreSQL instalada en el host remoto es 8.4.x anterior a 8.4.17, 9.0.x anterior a 9.0.13, 9.1.x anterior a 9.1.9 o 9.2.x anterior a 9.2.4. Por lo tanto, se ve potencialmente afectado por múltiples vulnerabilidades: - Los instaladores de Enterprise DB para Linux y Mac OS X crean un directorio y un archivo en '/tmp' con nombres predecibles. (CVE-2013-1902) - Los instaladores de Enterprise DB para Linux y Mac OS X pasan la contraseña de superusuario de la base de datos a un script de forma insegura. (CVE-2013-1903)
Solución	Actualice a PostgreSQL 8.4.17/9.0.13/9.1.9/9.2.4 o posterior.
Código Aplicaciones Afectadas	APP002, APP023, APP080, APP084

Vulnerabilidad	PostgreSQL Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su número de versión autoinformado, ya no se admite la instalación de PostgreSQL en el host remoto. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Upgrade to a version of PostgreSQL that is currently supported.
Código Aplicaciones Afectadas	APP002, APP023, APP080, APP084

Vulnerabilidad	Security Updates for Microsoft SQL Server 2016 and 2017 x64 (August 2018) (uncredentialed check)
Riesgo	Crítico
Descripción	Al servidor Microsoft SQL Server le falta una actualización de seguridad. Por lo tanto, se ve afectado por la vulnerabilidad de desbordamiento de búfer que permitiría la ejecución remota de código en un sistema afectado.

	Un atacante que aproveche con éxito la vulnerabilidad podría ejecutar código en el contexto de la cuenta de servicio del motor de base de datos de SQL Server.
Solución	Microsoft ha lanzado un conjunto de parches para las versiones x64 de SQL Server 2016 y 2017.
Código Aplicaciones Afectadas	APP071, APP304

Vulnerabilidad	SSL Version 2 and 3 Protocol Detection
Riesgo	Crítico
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. Un atacante puede aprovechar estas fallas para realizar ataques de man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo. NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía sólida" de PCI SSC.
Solución	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	Unsupported Windows OS (remote)
Riesgo	Crítico
Descripción	El sistema operativo remoto o el paquete de servicio ya no son compatibles.
Solución	Actualice a un paquete de servicio o sistema operativo compatible.
Código Aplicaciones Afectadas	APP122

Tabla 13. Vulnerabilidades Críticas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre.

4.4.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad (x6)	- Apache 2.4.x < 2.4.39 Multiple Vulnerabilities - Apache 2.4.x < 2.4.46 Multiple Vulnerabilities - Apache 2.4.x < 2.4.47 Multiple Vulnerabilities - Apache < 2.4.49 Multiple Vulnerabilities - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities - Apache 2.4.x < 2.4.52 Multiple Vulnerabilities

Riesgo	Alto
Descripción	Según su banner, la versión de Apache que se ejecuta en el host remoto se ve afectado por varias vulnerabilidades.
Solución	Actualice a la versión de Apache 2.4.53 o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	Firewall UDP Packet Source Port 53 Ruleset Bypass
Riesgo	Alto
Descripción	Es posible eludir las reglas del firewall remoto enviando paquetes UDP con un puerto de origen igual a 53. Un atacante puede usar esta falla para inyectar paquetes UDP a los hosts remotos, a pesar de la presencia de un firewall.
Solución	Póngase en contacto con el proveedor para obtener una actualización o revise la configuración de las reglas del cortafuegos.
Código Aplicaciones Afectadas	APP051, APP108, APP126, APP136, APP147

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.
Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP057, APP078, APP079, APP107, APP257, APP269

Vulnerabilidad	MS15-058: Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718) (uncredentialed check)
Riesgo	Alto
Descripción	La instalación remota de Microsoft SQL Server se ve afectada por múltiples vulnerabilidades: - Existe una vulnerabilidad de escalada de privilegios debido a la conversión de punteros a una clase incorrecta. Un atacante remoto autenticado puede explotar esto, a través de una consulta SQL especialmente diseñada, para obtener privilegios elevados. (CVE-2015-1761). - Existe una vulnerabilidad de ejecución remota de código debido al manejo incorrecto de llamadas de funciones internas a la memoria no inicializada. Un atacante puede explotar esto, a través de una consulta SQL especialmente diseñada en un servidor SQL afectado que tiene activada una configuración de permisos especiales (como VER ESTADO DEL SERVIDOR), para ejecutar código arbitrario. (CVE-2015-1762) - Existe una vulnerabilidad de ejecución remota de código debido al manejo incorrecto de llamadas de funciones internas a la memoria no inicializada. Un atacante remoto autenticado puede explotar esto, a través de una consulta SQL especialmente diseñada para ejecutar una función virtual desde una dirección incorrecta, para ejecutar código arbitrario. (CVE-2015-1762)
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2008, 2008 R2, 2012 y 2014.
Código Aplicaciones Afectadas	APP157, APP158

Vulnerabilidad (x4)	- MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows - MySQL < 5.0.83 Denial of Service - MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU) - MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.0.90 / 5.1.43 / 5.5.69 o posterior.
Código Aplicaciones Afectadas	APP051, APP105, APP108, APP126, APP136, APP147

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1l Vulnerability
Riesgo	Alto
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1l. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1l. - Para descifrar los datos cifrados de SM2, se espera que una aplicación llame a la función API EVP_PKEY_decrypt(). Normalmente, una aplicación llamará a esta función dos veces. La primera vez, al ingresar, el parámetro de salida puede ser NULL y, al salir, el parámetro de salida se completa con el tamaño de búfer necesario para contener el texto sin formato descifrado. Luego, la aplicación puede asignar un búfer de tamaño suficiente y volver a llamar a EVP_PKEY_decrypt(), pero esta vez pasando un valor no NULL para el parámetro de salida. Un error en la implementación del código de descifrado SM2 significa que el cálculo del tamaño del búfer necesario para contener el texto sin formato devuelto por la primera llamada a EVP_PKEY_decrypt() puede ser menor que el tamaño real requerido por la segunda llamada. Esto puede provocar un desbordamiento del búfer cuando la aplicación llama a EVP_PKEY_decrypt() por segunda vez con un búfer demasiado pequeño. Un atacante malintencionado que pueda presentar contenido SM2 para descifrarlo en una aplicación podría hacer que los datos elegidos por el atacante desborden el búfer hasta un máximo de 62 bytes alterando el contenido de otros datos retenidos después del búfer, posiblemente cambiando el comportamiento de la aplicación o causando que la aplicación chocar. La ubicación del búfer depende de la aplicación, pero normalmente se asigna en montón. Corregido en OpenSSL 1.1.1l (Afectado 1.1.1-1.1.1k). (CVE-2021-3711). - Las cadenas ASN.1 se representan internamente dentro de OpenSSL como una estructura ASN1_STRING que contiene un búfer que contiene los datos de la cadena y un campo que contiene la longitud del búfer. Esto contrasta con las cadenas C normales que se representan como un búfer para los datos de cadena que terminan con un byte NUL (0). Aunque no es un requisito estricto, las cadenas ASN.1 que se analizan usando las propias funciones d2i de OpenSSL (y otras funciones de análisis similares), así como cualquier cadena cuyo valor se haya establecido con la función ASN1_STRING_set(), además, terminará con NUL la matriz de bytes en el Estructura ASN1_STRING. Sin embargo, es posible que las aplicaciones construyan directamente estructuras ASN1_STRING válidas que no terminan en NUL la matriz de bytes configurando directamente los campos de datos y longitud en la matriz ASN1_STRING. Esto también puede suceder usando la función ASN1_STRING_set0(). Se ha encontrado que numerosas funciones de OpenSSL que imprimen datos ASN.1 asumen que la matriz de bytes ASN1_STRING terminará en NUL, aunque esto no está garantizado para cadenas que se construyeron directamente. Cuando una aplicación solicita que se imprima una estructura ASN.1 y esa estructura ASN.1 contiene ASN1_STRING que ha construido directamente la aplicación sin que NUL termine el campo de datos, entonces puede ocurrir una saturación del búfer de lectura. Lo mismo puede ocurrir durante el procesamiento de certificados de restricciones de nombre (por ejemplo, si la aplicación ha construido directamente un certificado en lugar de cargarlo a través de las funciones de análisis de OpenSSL, y el certificado contiene estructuras ASN1_STRING que no terminan en NUL). También puede ocurrir en las funciones X509_get1_email(), X509_REQ_get1_email() y X509_get1_ocsp(). Si un actor malicioso puede hacer que una aplicación construya directamente un ASN1_STRING y luego lo procese a través de una de las funciones OpenSSL afectadas, entonces este problema podría verse afectado. Esto podría provocar un bloqueo (lo que provocaría un ataque de denegación de servicio).

	También podría dar lugar a la divulgación de contenidos de la memoria privada (como claves privadas o texto sin formato confidencial). Corregido en OpenSSL 1.1.1l (Afectado 1.1.1-1.1.1k). Corregido en OpenSSL 1.0.2za (Afectado 1.0.2-1.0.2y). (CVE-2021-3712).
Solución	Actualice a OpenSSL versión 1.1.1l o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad (x8)	- Oracle Database Multiple Vulnerabilities (January 2016 CPU) - Oracle Database Multiple Vulnerabilities (April 2016 CPU) - Oracle Database Multiple Vulnerabilities (October 2017 CPU) - Oracle Database Multiple Vulnerabilities (April 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2015 CPU) - Oracle Database Multiple Vulnerabilities (October 2014 CPU) - Oracle Database Multiple Vulnerabilities (January 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente a la vulnerabilidad reportada.
Código Aplicaciones Afectadas	APP002, APP005, APP010, APP012, APP014, APP015, APP017, APP018, APP019, APP022, APP023, APP025, APP026, APP032, APP033, APP034, APP035, APP038, APP044, APP054, APP055, APP058, APP058, APP080, APP084, APP104, APP108, APP110, APP111, APP113, APP114, APP123, APP125, APP155, APP173, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP214, APP227, APP233, APP234, APP235, APP237, APP241, APP244, APP246, APP254, APP258, APP262, APP265, APP266, APP295

Vulnerabilidad (x5)	- PostgreSQL 9.2.x < 9.2.20 / 9.3.x < 9.3.16 / 9.4.x < 9.4.11 / 9.5.x < 9.5.6 / 9.6.x < 9.6.2 Multiple Vulnerabilities - PostgreSQL 9.1.x < 9.1.24 / 9.2.x < 9.2.19 / 9.3.x < 9.3.15 / 9.4.x < 9.4.10 / 9.5.x < 9.5.5 / 9.6.x < 9.6.1 Aggregate Functions Use-after-free DoS - PostgreSQL 9.0 < 9.0.20 / 9.1 < 9.1.16 / 9.2 < 9.2.11 / 9.3 < 9.3.7 / 9.4 < 9.4.2 Multiple Vulnerabilities - PostgreSQL 9.1.x < 9.1.20 / 9.2.x < 9.2.15 / 9.3.x < 9.3.11 / 9.4.x < 9.4.6 / 9.5.x < 9.5.1 Multiple Vulnerabilities - PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Predictable Random Number Generator
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a PostgreSQL versión 9.2.20/9.3.16/9.4.11/9.5.6/9.6.2 o posterior.
Código Aplicaciones Afectadas	APP002, APP023, APP080, APP084

Vulnerabilidad	Unsupported Web Server Detection
Riesgo	Alto
Descripción	Según su versión, el servidor web está obsoleto y su proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.
Solución	Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.
Código Aplicaciones Afectadas	APP122

Tabla 14. Vulnerabilidades Altas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre.

4.4.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad (x12)	- Apache 2.4.x < 2.4.38 Multiple Vulnerabilities - Apache 2.4.x < 2.4.38 Multiple Vulnerabilities - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities - Apache < 2.4.49 Multiple Vulnerabilities - Apache < 2.4.49 Multiple Vulnerabilities - Apache >= 2.4.17 < 2.4.49 mod_http2 - Apache >= 2.4.17 < 2.4.49 mod_http2 - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi
Riesgo	Medio
Descripción	El servidor web remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache 2.4.49 o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	Apache ServerTokens Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor, el sistema operativo y las versiones del módulo.
Solución	Cambie el valor de configuración de Apache ServerTokens a 'Prod'
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	HTTP TRACE / TRACK Methods Allowed
Riesgo	Medio
Descripción	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Solución	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS

Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103

Vulnerabilidad (x10)	- MariaDB 10.1.x < 10.1.42 Denial Of Service Vulnerability - MariaDB 10.1.0 < 10.1.44 A Vulnerability - MariaDB 10.1.0 < 10.1.39 Multiple Vulnerabilities - MariaDB 10.1.0 < 10.1.45 Multiple Vulnerabilities - MariaDB 10.3.x < 10.3.19 Multiple Denial of Service Vulnerabilities - MariaDB 10.3.0 < 10.3.22 A Vulnerability - MariaDB 10.3.0 < 10.3.23 Multiple Vulnerabilities - MariaDB 10.3.0 < 10.3.13 Multiple Vulnerabilities - MariaDB 10.3.0 < 10.3.17 Multiple Vulnerabilities - MariaDB 10.3.0 < 10.3.15 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MariaDB versión 5.5.68, 10.0.30, 10.1.45, 10.2.5, 10.3.23 o posterior.
Código Aplicaciones Afectadas	APP131, APP248, APP249, APP251, APP252

Vulnerabilidad	MS11-049: Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893) (uncredentialed check)
Riesgo	Medio
Descripción	Una aplicación en el host remoto tiene una vulnerabilidad de divulgación de información. Al analizar un archivo de detección de servicios web (.disco) especialmente diseñado, se permiten entidades XML externas para la entrada de usuarios que no son de confianza. Un atacante remoto explotaría esto engañando a un usuario para que abra un archivo .disco especialmente diseñado, lo que resultaría en la divulgación de información confidencial.
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2005, 2008 y 2008 R2.
Código Aplicaciones Afectadas	APP122

Vulnerabilidad	MS16-136: Security Update for SQL Server (3199641) (uncredentialed check)
Riesgo	Medio
Descripción	Al Microsoft SQL Server remoto le falta una actualización de seguridad. Está, por tanto, afectado por múltiples vulnerabilidades: - Existen múltiples vulnerabilidades de elevación de privilegios en el motor SQL RDBMS debido al manejo inadecuado de la conversión de punteros. Un atacante remoto autenticado puede aprovecharlos para obtener privilegios elevados. (CVE-2016-7249, CVE-2016-7250, CVE-2016-7254) - Existe una vulnerabilidad de secuencias de comandos entre sitios (XSS) en la API de MDS del servidor SQL debido a una validación incorrecta de un parámetro de solicitud en el sitio del servidor SQL. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud especialmente diseñada, para ejecutar código arbitrario en la sesión del navegador del usuario. (CVE-2016-7251)

	- Existe una vulnerabilidad de divulgación de información en Microsoft SQL Analysis Services debido a una validación incorrecta de la ruta de FILESTREAM. Un atacante remoto autenticado puede explotar esto para revelar información confidencial de archivos y bases de datos. (CVE-2016-7252) - Existe una vulnerabilidad de elevación de privilegios en Microsoft SQL Server Engine debido a una verificación incorrecta por parte del Agente SQL Server de las ACL en atxcore.dll. Un atacante remoto autenticado puede explotar esto para obtener privilegios elevados. (CVE-2016-7253)
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2012, 2014 y 2016.
Código Aplicaciones Afectadas	APP157, APP158

Vulnerabilidad (x12)	- MySQL < 5.0.92 Multiple Denial of Service - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities - MySQL 5.0 < 5.0.88 Multiple Vulnerabilities - MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass - MySQL 5.1.x < 5.7.3 SSL/TLS Downgrade MitM (BACKRONYM) - MySQL 5.5.x < 5.5.54 Multiple Vulnerabilities (January 2017 CPU) - MySQL 5.5.x < 5.5.55 Multiple Vulnerabilities (April 2017 CPU) (Riddle) - MySQL 5.5.x < 5.5.57 Multiple Vulnerabilities (July 2017 CPU) - MySQL 5.5.x < 5.5.58 Multiple Vulnerabilities (October 2017 CPU) - MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU) - MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU) - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de MySQL 5.0 instalada en el host remoto se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a MySQL versión 5.0.95, 5.7.3, 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP002, APP023, APP051, APP080, APP084, APP105, APP108, APP126, APP136, APP147

Vulnerabilidad	MySQL Binary Log SQL Injection
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host es anterior a 5.5.33 / 5.6.x anterior a 5.6.13 y, por lo tanto, está potencialmente afectada por múltiples vulnerabilidades de inyección de SQL. Los identificadores proporcionados por el usuario no se citan correctamente antes de escribirse en el registro binario. Un atacante con una cuenta válida y privilegios para modificar puede modificar tablas a las que no debería tener acceso.
Solución	Actualice a MySQL versión 5.5.33 / 5.6.13 o posterior.
Código Aplicaciones Afectadas	APP002, APP023, APP051, APP080, APP084, APP108, APP126, APP136, APP147

Vulnerabilidad	MySQL Denial of Service (Jul 2020 CPU)
Riesgo	Medio
Descripción	La versión de MySQL que se ejecuta en el host es menor a 5.7.29 o menor a 8.0.19. Por lo tanto, se ve afectado por una vulnerabilidad, como se indica en el aviso de actualización del parche crítico de julio de 2020: Una vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Servidor: Replicación). Las versiones compatibles que se ven afectadas son menores a 5.7.29 y menores a 8.0.19. La vulnerabilidad fácilmente explotable permite que un atacante con muchos privilegios con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server.

Solución	Consulte el aviso del proveedor.
Código Aplicaciones Afectadas	APP002, APP023, APP051 APP080, APP084, APP105, APP108, APP126, APP136, APP147

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión del producto probado instalado en el host remoto es anterior a la versión probada
Solución	Actualice a OpenSSL versión 1.1.1d o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1e-dev. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1e-dev.
Solución	Actualice a OpenSSL versión 1.1.1e-dev o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability
Riesgo	Medio
Descripción	La versión del producto probado instalado en el host remoto es anterior a la versión probada. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1i.
Solución	Actualice a OpenSSL versión 1.1.1i o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1j Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1j. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 1.1.1j.
Solución	Actualice a OpenSSL versión 1.1.1jo posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1k Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1k. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 1.1.1k.
Solución	Actualice a OpenSSL versión 1.1.1k o posterior.

Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1m Vulnerability
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a la 1.1.1m. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1m.
Solución	Actualice a OpenSSL versión 1.1.1m o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad	OpenSSL 1.1.1 < 1.1.1n Vulnerability
Riesgo	Medio
Descripción	La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1n. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1n.
Solución	Actualice a OpenSSL versión 1.1.1n o posterior.
Código Aplicaciones Afectadas	APP328

Vulnerabilidad (x5)	- Oracle Database Multiple Vulnerabilities (April 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2018 CPU) - Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32) - Oracle Database Multiple Vulnerabilities (October 2016 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente al anuncio de la vulnerabilidad.
Código Aplicaciones Afectadas	APP002, APP005, APP010 APP012, APP014, APP015, APP017, APP018, APP019, APP022, APP023, APP025, APP026, APP032, APP033, APP034, APP035, APP038, APP044, APP054, APP055, APP058, APP058, APP080, APP084, APP104, APP108, APP110, APP111, APP113, APP114, APP123, APP125, APP155, APP173, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP214, APP227, APP233, APP234, APP235, APP237, APP241, APP244, APP246, APP254. APP258, APP262, APP265, APP266, APP295

Vulnerabilidad	Oracle Database Server CVE-2018-3110
Riesgo	Medio
Descripción	Faltan parches en el Oracle Database Server remoto. Está, por tanto, afectado por CVE-2018-3110.
Solución	Aplique el parche adecuado de acuerdo con el aviso de alerta de seguridad de Oracle - CVE-2018-3110.
Código Aplicaciones Afectadas	APP002, APP005, APP010, APP012, APP014, APP015, APP017, APP018, APP019, APP022, APP023, APP025, APP026, APP032, APP033, APP034, APP035, APP038, APP044, APP054, APP055, APP058, APP058, APP080, APP084, APP104, APP108, APP110, APP111, APP113, APP114, APP123, APP125, APP155, APP173, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP214, APP227, APP233, APP234, APP235, APP237, APP241, APP244, APP246, APP254, APP258, APP262, APP265, APP266, APP295

Vulnerabilidad	Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos de Oracle remoto no tiene la actualización de parche crítico (CPU) de abril de 2018. Por lo tanto, se ve afectado por una vulnerabilidad de ejecución remota de código, como se indica en el aviso de actualización de parche crítico de abril de 2018. Consulte los detalles de CVRF para los CVE aplicables para obtener información adicional.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018.
Código Aplicaciones Afectadas	APP002, APP005, APP010, APP012, APP014, APP015, APP017, APP018, APP019, APP022, APP023, APP025, APP026, APP032, APP033, APP034, APP035, APP038, APP044, APP054, APP055, APP058, APP058, APP080, APP084, APP104, APP108, APP110, APP111, APP113, APP114, APP123, APP125, APP155, APP173, APP174, APP175, APP178, APP180, APP181, APP183, APP184, APP188, APP189, APP190, APP209, APP211, APP214, APP227, APP233, APP234, APP235, APP237, APP241, APP244, APP246, APP254, APP258, APP262, APP265, APP266, APP295

Vulnerabilidad (x8)	- PHP 7.3.x < 7.3.25 / 7.4.x < 7.4.13 Multiple Vulnerabilities - PHP 7.4.x < 7.4.12 DoS - PHP 7.4.x < 7.4.25 - PHP 7.4.x < 7.4.26 - PHP 7.4.x < 7.4.28 - PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error - PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS - PHP 7.4.x < 7.4.18 / 8.x < 8.0.5 Integer Overflow
Riesgo	Medio
Descripción	La versión de PHP instalada en el host, se ve afectado por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a la versión de PHP 7.3.27, 7.4.18, 8.0.5 o posterior.
Código Aplicaciones Afectadas	APP327

Vulnerabilidad (x8)	- PostgreSQL 9.3 < 9.3.23 / 9.4 < 9.4.18 / 9.5 < 9.5.13 / 9.6 < 9.6.9 / 10.3 Insecure ACL Remote Issue - PostgreSQL 8.3 < 8.3.23 / 8.4 < 8.4.16 / 9.0 < 9.0.12 / 9.1 < 9.1.8 / 9.2 < 9.2.3 Denial of Service - PostgreSQL 8.4 < 8.4.20 / 9.0 < 9.0.16 / 9.1 < 9.1.12 / 9.2 < 9.2.7 / 9.3 < 9.3.3 Multiple Vulnerabilities - PostgreSQL 9.0 < 9.0.19 / 9.1 < 9.1.15 / 9.2 < 9.2.10 / 9.3 < 9.3.6 / 9.4 < 9.4.1 Multiple Vulnerabilities - PostgreSQL 9.0.x < 9.0.23 / 9.1.x < 9.1.19 / 9.2.x < 9.2.14 / 9.3.x < 9.3.10 / 9.4.x < 9.4.5 Multiple Vulnerabilities - PostgreSQL 9.1.x < 9.1.23 / 9.2.x < 9.2.18 / 9.3.x < 9.3.14 / 9.4.x < 9.4.9 / 9.5.x < 9.5.4 Multiple Vulnerabilities - PostgreSQL 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 File Deletion - PostgreSQL 9.1 < 9.1.9 / 9.2 < 9.2.4 Denial of Service
Riesgo	Medio
Descripción	La versión de PHP instalada en el host, se ve afectado por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a PostgreSQL 9.3.23/9.4.18/9.5.13/9.6.9/10.4 o posterior.
Código Aplicaciones Afectadas	APP002, APP023, APP080, APP084

Vulnerabilidad	Security Updates for Microsoft SQL Server (May 2019)
Riesgo	Medio

Descripción	A la instalación de Microsoft SQL Server le falta una actualización de seguridad. Por lo tanto, se ve afectado por una vulnerabilidad de divulgación de información que existe en Microsoft SQL Server Analysis Services cuando aplica incorrectamente los permisos de metadatos. Un atacante que aproveche con éxito la vulnerabilidad podría consultar tablas o columnas para las que no tiene derechos de acceso.
Solución	Microsoft ha publicado las siguientes actualizaciones de seguridad para solucionar este problema: - KB4494352 - KB4494351
Código Aplicaciones Afectadas	APP304

Vulnerabilidad	Security Updates for Microsoft SQL Server (Uncredentialed Check) (February 2020)
Riesgo	Medio
Descripción	A la instalación de Microsoft SQL Server en el host le falta una actualización de seguridad. Por tanto, se ve afectado por la siguiente vulnerabilidad: - Existe una vulnerabilidad de ejecución remota de código en Microsoft SQL Server Reporting Services cuando maneja incorrectamente las solicitudes de página. Un atacante que aproveche con éxito esta vulnerabilidad podría ejecutar código en el contexto de la cuenta de servicio del servidor de informes. (CVE-2020-0618)
Solución	Microsoft ha publicado las siguientes actualizaciones de seguridad para solucionar este problema: -KB4532095 -KB4532097 -KB4532098 -KB4535288 -KB4535706
Código Aplicaciones Afectadas	APP071, APP041

Vulnerabilidad	Security Updates for Microsoft SQL Server (Uncredentialed Check) (July 2019)
Riesgo	Medio
Descripción	A la instalación de Microsoft SQL Server le falta una actualización de seguridad. Por lo tanto, se ve afectado por la siguiente vulnerabilidad: - Ejecución remota de código en Microsoft SQL Server cuando maneja incorrectamente el procesamiento de funciones internas. Un atacante que aproveche con éxito esta vulnerabilidad podría ejecutar código en el contexto de la cuenta de servicio del motor de base de datos de SQL Server. (CVE-2019-1068)
Solución	Microsoft ha publicado las siguientes actualizaciones de seguridad para solucionar este problema: - KB4505217 - KB4505419 - KB4505422 - KB4505218 - KB4505219 - KB4505225 - KB4505224 - KB4505222 - KB4505221 - KB4505220
Código Aplicaciones Afectadas	APP304

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloque con bloques de 64 bits en uno o más conjuntos de cifrado. Por lo tanto, se ve afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de cifrados de bloque débiles de 64 bits. Un atacante intermediario que tenga suficientes recursos puede explotar esta vulnerabilidad, a través de un ataque de 'birthday', para detectar una colisión que filtre el XOR entre el secreto fijo y un texto plano conocido, permitiendo la divulgación del texto secreto, como las cookies HTTPS seguras, y posiblemente resulte en el secuestro de una sesión autenticada.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloque de 64 bits. Alternativamente, establezca limitaciones en la cantidad de solicitudes que se pueden procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Código Aplicaciones Afectadas	APP041, APP122, APP318

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP039, APP041, APP057, APP071, APP078, APP079, APP107, APP122, APP157, APP158, APP230, APP236, APP245, APP260, APP260, APP283, APP283, APP296, APP297, APP298, APP300, APP304, APP318, APP328

Vulnerabilidad	SSL Certificate Expiry
Riesgo	Medio
Descripción	Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.
Solución	Compre o genere un nuevo certificado SSL para reemplazar el existente.
Código Aplicaciones Afectadas	APP245

Vulnerabilidad	SSL Certificate Signed Using Weak Hashing Algorithm
Riesgo	Medio
Descripción	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Solución	Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL.
Código Aplicaciones Afectadas	APP039, APP041, APP057, APP071, APP078, APP079, APP107, APP122, APP157, APP158, APP230, APP236, APP260, APP260, APP260, APP283, APP283, APP296, APP297, APP298, APP298, APP300

Vulnerabilidad	SSL Certificate with Wrong Hostname
Riesgo	Medio
Descripción	El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
Solución	Compre o genere un certificado SSL adecuado para este servicio.

Código Aplicaciones Afectadas	APP039, APP041, APP071, APP122, APP157, APP158, APP230, APP236, APP260, APP260, APP267, APP283, APP296, APP297, APP298, APP300, APP304

Vulnerabilidad	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Riesgo	Medio
Descripción	El host remoto admite SSLv2 y, por lo tanto, puede verse afectado por una vulnerabilidad que permite un ataque de Oracle de relleno Bleichenbacher entre protocolos conocido como DROWN (Descifrado de RSA con cifrado obsoleto y debilitado). Esta vulnerabilidad existe debido a una falla en la implementación de Secure Sockets Layer Versión 2 (SSLv2), y permite descifrar el tráfico TLS capturado. Un atacante man-in-the-middle puede aprovechar esto para descifrar la conexión TLS utilizando tráfico capturado previamente y criptografía débil junto con una serie de conexiones especialmente diseñadas a un servidor SSLv2 que usa la misma clave privada.
Solución	Deshabilite SSLv2 y los conjuntos de cifrado de criptografía de grado de exportación. Asegúrese de que las claves privadas no se utilicen en ningún lugar con software de servidor que admita conexiones SSLv2.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	SSL Medium Strength Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Código Aplicaciones Afectadas	APP041, APP122, APP318

Vulnerabilidad	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Riesgo	Medio
Descripción	El host admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en la generación de un flujo de bytes pseudoaleatorio, por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP039, APP041, APP057, APP071, APP078, APP079, APP107, APP122, APP157, APP158, APP230, APP236, APP260, APP283, APP296, APP297, sAPP298, APP300, APP304, APP318, APP328

Vulnerabilidad	SSL Weak Cipher Suites Supported
Riesgo	Medio
Descripción	El host remoto admite el uso de cifrados SSL que ofrecen un cifrado débil.
Solución	Reconfigure la aplicación afectada, si es posible para evitar el uso de cifrados débiles.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Riesgo	Medio
Descripción	El host se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados mediante cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC). Los atacantes MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas. Siempre que un cliente y un servicio sean compatibles con SSLv3, una conexión se puede "revertir" a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o una versión posterior. El mecanismo TLS Fallback SCSV evita los ataques de "reversión de versiones" sin afectar a los clientes heredados; sin embargo, solo puede proteger las conexiones cuando el cliente y el servicio admiten el mecanismo. Los sitios que no pueden deshabilitar SSLv3 de inmediato deben habilitar este mecanismo. Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación de SSL en particular. Desactivar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.
Solución	Desactive SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda inhabilitar SSLv3.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP003, APP008, APP021, APP030, APP039, APP041, APP047, APP057, APP071, APP073, APP074, APP078, APP079, APP087, APP088, APP089, APP107, APP119, APP120, APP121, APP122, APP156, APP157, APP158, APP230, APP236, APP256, APP260, APP266, APP267, APP277, APP283, APP296, APP297, APP298, APP300, APP304, APP318, APP322

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

Código Aplicaciones Afectadas	APP003, APP008, APP021, APP030, APP039, APP041, APP047, APP057, APP071, APP073, APP074, APP078, APP079, APP087, APP088, APP089, APP107, APP119, APP120, APP121, APP122, APP156, APP157, APP158, APP230, APP236, APP256, APP256, APP257, APP260, APP266, APP267, APP277, APP283, APP296, APP297, APP298, APP300, APP304, APP318, APP322

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique los encabezados HTTP del servidor web para no revelar información detallada sobre el servidor web subyacente.
Código Aplicaciones Afectadas	APP328, APP122

Tabla 15. Vulnerabilidades Medias sobre IP servidores de bases de datos de los sistemas definidos para el 6to trimestre.

4.4.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	MariaDB 10.1.0 < 10.1.41 Multiple Vulnerabilities
Riesgo	Bajo
Descripción	La versión de MariaDB instalada en el host remoto es anterior a la 10.1.41. Por lo tanto, se ve afectado por las siguientes vulnerabilidades, como se menciona en el aviso mdb-10141-rn. - Una vulnerabilidad en el 'Servidor: Autenticación conectable' subcomponente Esta es una vulnerabilidad fácilmente explotable que permite que un atacante altamente privilegiado con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o bloqueo repetible (DOS completo) del servidor MariaDB. (CVE-2019-2737) - Una vulnerabilidad en el 'Servidor: Seguridad: Privilegios' subcomponente Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con muchos privilegios, que puede iniciar sesión en la infraestructura donde se ejecuta el servidor MariaDB, comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) del servidor MariaDB, así como la actualización, inserción o eliminación no autorizadas del acceso a algunos de los datos accesibles al servidor MariaDB. (CVE-2019-2739) - Una vulnerabilidad en el subcomponente 'Servidor: XML'. Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa un servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o falla repetible (DOS completo) de MariaDB Servidor. (CVE-2019-2740) - Una vulnerabilidad en el subcomponente 'Server: Parser'. Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o bloqueo repetible (DOS completo) del servidor MariaDB. (CVE-2019-2805)
Solución	Actualice a MariaDB versión 10.1.41 o posterior
Código Aplicaciones Afectadas	APP248, APP249, APP251

Vulnerabilidad	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
Riesgo	Bajo
Descripción	La versión de MySQL instalada en el host remoto es anterior a 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 y, por lo tanto, no codifica correctamente los corchetes angulares cuando se usa la opción 'mysql --html'. Dependiendo de cómo se procese la salida del comando del cliente mysql, el usuario puede ser vulnerable a ataques de secuencias de comandos entre sitios.
Solución	Actualice a MySQL versión 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP051, APP108, APP126, APP136, APP147

Vulnerabilidad	SSH Server CBC Mode Ciphers Enabled
Riesgo	Bajo
Descripción	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado del modo de cifrado CBC y habilitar el cifrado del modo de cifrado CTR o GCM.
Código Aplicaciones Afectadas	APP243, APP303

Vulnerabilidad	SSL Anonymous Cipher Suites Supported
Riesgo	Bajo
Descripción	El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite a un administrador configurar un servicio que cifra el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de man-in-the-middle.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados débiles.
Código Aplicaciones Afectadas	APP041, APP122

Vulnerabilidad	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Riesgo	Bajo
Descripción	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave de menos de 2048 bits. De acuerdo con los estándares de la industria establecidos por el foro de la autoridad de certificación/navegador (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048 bits. Algunas implementaciones SSL de navegador pueden rechazar claves de menos de 2048 bits después del 1 de enero de 2014. Además, algunos proveedores de certificados SSL pueden revocar certificados de menos de 2048 bits antes del 1 de enero de 2014
Solución	Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga y vuelva a emitir cualquier certificado firmado por el certificado anterior.
Código Aplicaciones Afectadas	APP041, APP122, APP157, APP158

Vulnerabilidad	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Riesgo	Bajo

Descripción	El host admite conjuntos de cifrado EXPORT_DHE con claves menores o iguales a 512 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en poco tiempo. Un atacante man-in-the-middle puede degradar la sesión para usar conjuntos de cifrado EXPORT_DHE. Por lo tanto, se recomienda eliminar el soporte para conjuntos de cifrado débiles.
Solución	Vuelva a configurar el servicio para eliminar la compatibilidad con los conjuntos de cifrado EXPORT_DHE.
Código Aplicaciones Afectadas	APP041, APP122

Tabla 16. Vulnerabilidades Bajas sobre IP servidores de bases de datos de producción de los sistemas definidos para el 6to trimestre.

5. RESUMEN EJECUTIVO CRITICIDAD DE LAS VULNERABILIDADES IDENTIFICADAS

La criticidad de las diferentes vulnerabilidades detectadas en las aplicaciones seleccionadas del primer escenario, en donde se evaluaron los servidores de aplicación del ambiente de certificación, se resumen en la siguiente gráfica:

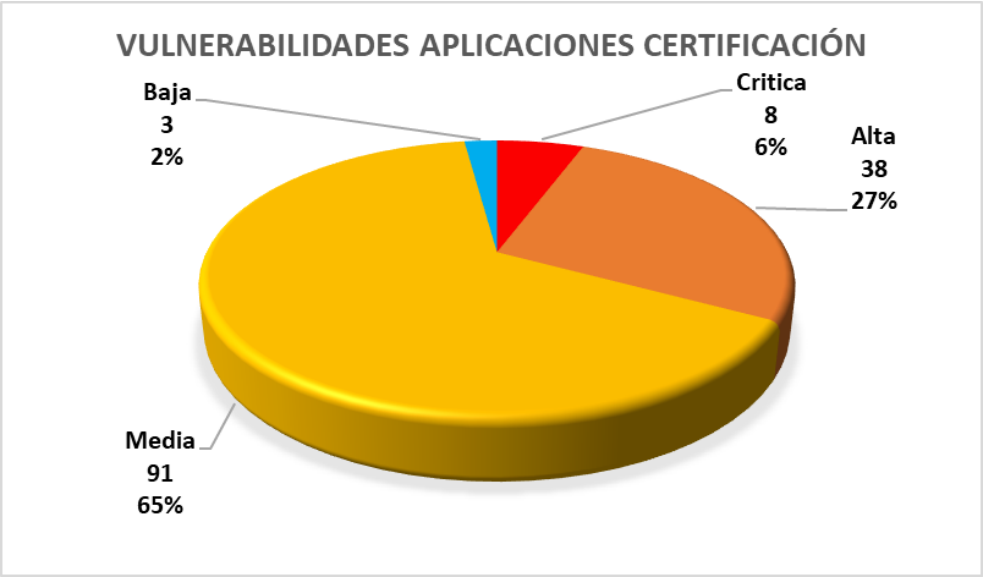

Ilustración 1. Criticidad de las vulnerabilidades detectadas para los servidores de las aplicaciones seleccionadas del ambiente de certificación con excepción.

De allí se observa que más de la mitad de las vulnerabilidades identificadas tienen una criticidad de nivel medio, seguido de vulnerabilidades de criticidad alta, critica y baja.

Para el caso de las vulnerabilidades distribuidas sobre los servidores de bases de datos en el ambiente de certificación, se tiene el siguiente resultado:

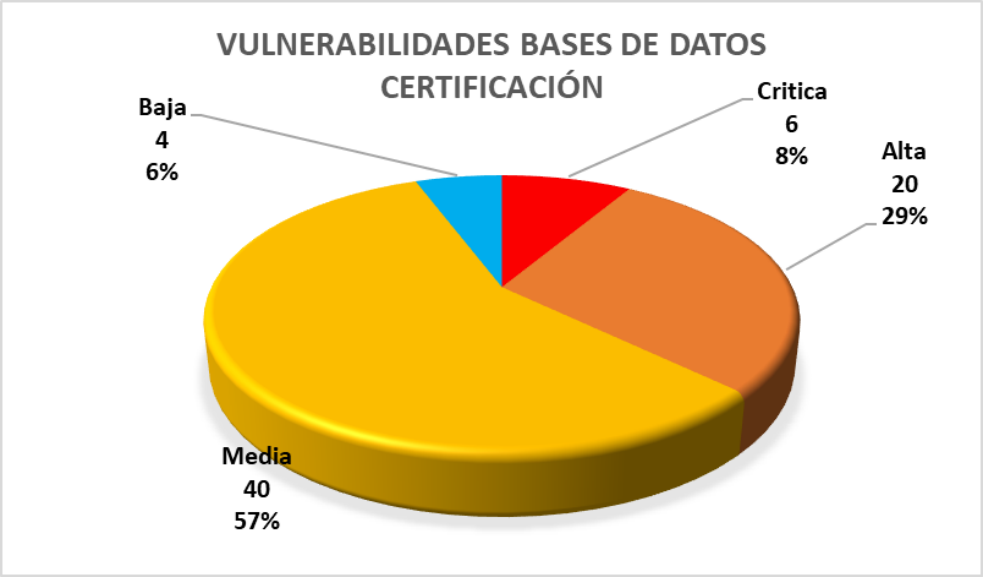

Ilustración 2. Criticidad de las vulnerabilidades detectadas para los servidores de bases de datos de las aplicaciones seleccionadas del ambiente de certificación.

Se presenta un caso similar en el sentido de que más de la mitad de las vulnerabilidades identificadas tienen una criticidad de nivel medio, seguido de vulnerabilidades de criticidad alta, critica y baja. La mayoría de ellas tienen que ver con el versionamiento a nivel de Oracle, por lo cual su mitigación depende en gran medida de que se puedan actualizar las plataformas de bases de datos.

Para los servidores que soportan las aplicaciones seleccionadas del ambiente de producción, las diferentes vulnerabilidades encontradas tienen la siguiente distribución de criticidad.

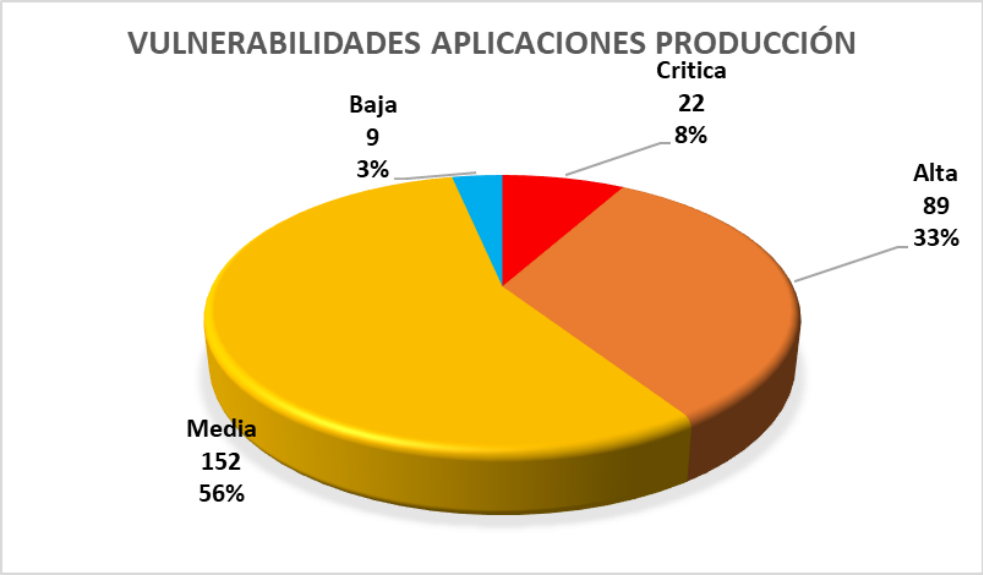

Ilustración 3. Criticidad de las vulnerabilidades detectadas para los servidores de las aplicaciones seleccionadas del ambiente de producción con excepción.

Sobre estos servidores se encuentra una mayoría de vulnerabilidades de severidad media principalmente relacionadas con la versión de capas medias como Apache y PHP. Incluso también aparecen en este apartado vulnerabilidades asociadas a componentes de bases de datos, dado que se detectan que sobre el servidor de aplicación también corre algún componente de este tipo.

En cuanto a lo obtenido a nivel de bases de datos para las aplicaciones de producción, se tiene también una mayoría de vulnerabilidades de criticidad media, seguida por vulnerabilidades de criticidad alta y critica como se puede ver en la siguiente imagen:

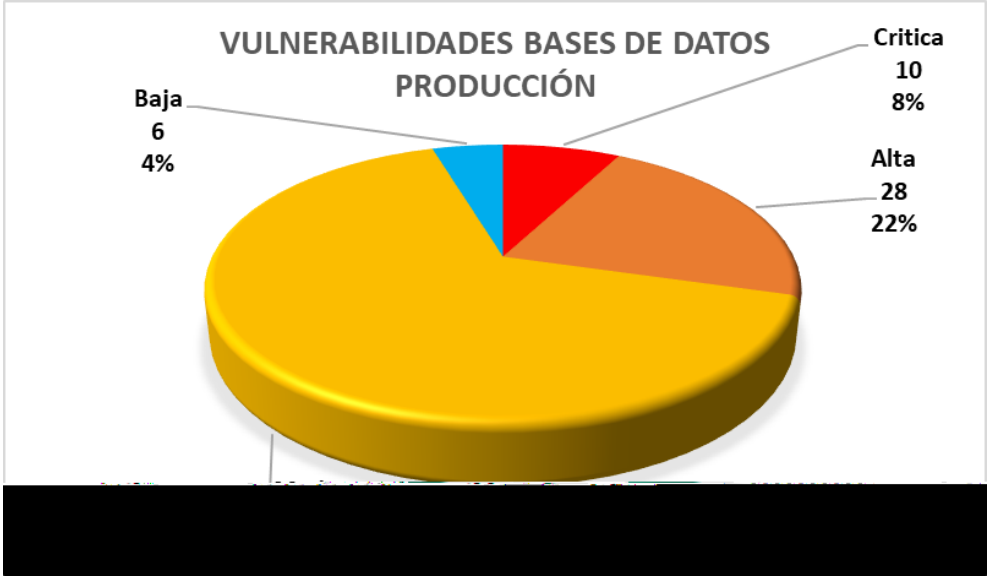

Ilustración 4. Criticidad de las vulnerabilidades detectadas para los servidores de bases de datos de las aplicaciones seleccionadas del ambiente de producción.

La mayoría de las vulnerabilidades representadas por las versiones detectadas de MariaDB, MySQL y Oracle y cuya mitigación depende en gran medida de algún proceso de actualización.

6. CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el proceso de escaneo y análisis de vulnerabilidades se presentan las siguientes conclusiones y recomendaciones:

- Se identifican vulnerabilidades asociadas a la utilización de software con algún nivel de obsolescencia como versiones de PHP, Apache Tomcat, Apache, Oracle, MySQL, jquery, entre otros, ya que la utilización de versiones obsoletas es la que más genera vulnerabilidades. Por lo cual las vulnerabilidades que dependen principalmente por la detección de una versión en particular, dependen principalmente de un proceso de actualización.

- Se recomienda a los especialistas en su proceso de mitigación dar prioridad a la remediación de las vulnerabilidades para las cuales existen *exploits* disponible y que tienen nivel de riesgo Crítico y Alto, debido a que la probabilidad de ser explotadas es mayor y la materialización del riesgo representaría un impacto considerable.

- Se recomienda aislar a nivel de red los servidores y servicios con vulnerabilidades que no puedan ser remediadas, de modo que sólo puedan ser accedidos por los usuarios y/o sistemas autorizados.

7. ANEXOS

- Sistemas_Trimestre_6.xlsx
- RFC_10471_OC63260_SERV_APP_CERT.html
- RFC_10471_OC63260_SERV_APP_PROD.html
- RFC_10471_OC63260_SERV_BD_CERT.html
- RFC_10471_OC63260_SERV_BD_PROD.html

Información del documento

Fecha	Versión	Responsable	Revisado por	Aprobado por
27/04/2022	1.0	Especialista seguridad informática	Líder de Gestión técnica y seguridad	

Control de cambios

Fecha	Versión	Causa Cambio	Responsable
27/04/2022	1.0	Creación del Documento	Especialista seguridad informática