INFORME: VULNERABILIDADES TRIMESTRE 5

SERVICIOS TIC

MINISTERIO DE EDUCACIÓN NACIONAL

UNIÓN TEMPORAL GESTIÓN INTEGRAL MEN

Febrero de 2022

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. OBJETIVO

Presentar el resultado del escaneo y análisis de vulnerabilidades realizado durante el

	archivo de imagen con formato incorrecto a un usuario en el host y esperar a que lo abra usando una aplicación de Microsoft afectada.
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2000 y 2005.
Dispositivos Afectados	10.1.120.85-MEN317485

Vulnerabilidad	MS15-058: Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718) (uncredentialed check)
Riesgo	Alto
Descripción	La instalación 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.
Dispositivos Afectados	10.1.150.130-MEN317457

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 múltiples 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 explotar 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 explotar 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 divulgadas el 14/04/2017 por un grupo conocido como Shadow Brokers. WannaCry/WannaCrypt que 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 los sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8. Para sistemas operativos Windows no compatibles, por ejemplo Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1. SMBv1 carece de funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede deshabilitar 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 límite de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.
Dispositivos Afectados	10.1.100.22-MEN311015, 10.1.110.30-MEN307888, 10.1.5.89

Vulnerabilidad	Multiple BSD ipfw / ip6fw ECE Bit Filtering Evasion
Riesgo	Alto
Descripción	El host parece vulnerable a un error en el que un atacante remoto puede eludir el firewall configurando el bit ECE dentro del campo de indicadores TCP. Se sabe que al menos un firewall (ipfw) exhibe este tipo de comportamiento. Los sistemas vulnerables conocidos incluyen todos los FreeBSD 3.x, 4.x, 3.5-STABLE y 4.2-STABLE.
Solución	Si está ejecutando FreeBSD 3.X, 4.x, 3.5-STABLE, 4.2-STABLE, actualice su firewall. Si no está ejecutando FreeBSD, comuníquese con su proveedor de firewall para obtener un parche.
Dispositivos Afectados	10.1.4.126

Vulnerabilidad	nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities
Riesgo	Alto
Descripción	Según el encabezado 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.
Dispositivos Afectados	10.1.155.23

Vulnerabilidad	Oracle TNS Listener Remote Poisoning
Riesgo	Alto
Descripción	El servicio de Oracle TNS permite el registro de servicios desde un host remoto. Un atacante puede explotar este problema para desviar datos de un cliente o servidor de base de datos legítimo a un sistema especificado por el atacante. Las explotaciones exitosas permitirán que el atacante manipule las instancias de la base de datos, lo que podría facilitar 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 en el aviso de Oracle.
Dispositivos Afectados	10.1.155.23

Vulnerabilidad (x35)	PHP < 5.2.11 Multiple Vulnerabilities PHP < 5.2.8 Multiple Vulnerabilities PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

	PHP < 5.3.9 Multiple Vulnerabilities PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability. PHP 5 < 5.2.7 Multiple Vulnerabilities PHP 5.2 < 5.2.14 Multiple Vulnerabilities PHP 5.6.x < 5.6.12 Multiple Vulnerabilities PHP 5.6.x < 5.6.13 Multiple Vulnerabilities PHP 5.6.x < 5.6.19 Multiple Vulnerabilities PHP 5.6.x < 5.6.20 Multiple Vulnerabilities PHP 5.6.x < 5.6.21 Multiple Vulnerabilities PHP 5.6.x < 5.6.22 Multiple Vulnerabilities PHP 5.6.x < 5.6.23 Multiple Vulnerabilities PHP 5.6.x < 5.6.24 Multiple Vulnerabilities (httpoxy) PHP 5.6.x < 5.6.25 Multiple Vulnerabilities PHP 5.6.x < 5.6.26 Multiple Vulnerabilities PHP 5.6.x < 5.6.29 Multiple Vulnerabilities PHP 5.6.x < 5.6.30 Multiple DoS PHP 5.6.x < 5.6.31 Multiple Vulnerabilities PHP 5.6.x < 5.6.32 Multiple Vulnerabilities PHP 5.6.x < 5.6.34 Stack Buffer Overflow PHP 5.6.x < 5.6.39 Multiple vulnerabilities PHP 5.6.x < 5.6.40 Multiple vulnerabilities. PHP 5.6.x < 5.6.9 Multiple Vulnerabilities PHP 7.0.x < 7.0.19 Multiple Vulnerabilities PHP 7.0.x < 7.0.25 Multiple Vulnerabilities PHP 7.0.x < 7.0.28 Stack Buffer Overflow PHP 7.0.x < 7.0.31 Use After Free Arbitrary Code Execution in EXIF PHP 7.0.x < 7.0.33 Multiple vulnerabilities PHP 7.2.x < 7.2.13 Multiple vulnerabilities PHP 7.2.x < 7.2.14 Multiple vulnerabilities. PHP 7.2.x < 7.2.16 Multiple vulnerabilities. PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF PHP 7.3.x < 7.3.13 / 7.4.x < 7.4.1 Multiple Vulnerabilities
Riesgo	Alto
Descripción	La versión de PHP que se ejecuta en el host se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a la versión de PHP 7.2.24, 7.3.13, 7.4.1 o posterior.
Dispositivos Afectados	10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.100.30-MEN314492, 10.1.110.92-MEN317763, 10.1.5.103-MEN317763

Vulnerabilidad (x7)	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 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 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 9.2.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 9.2.x < 9.2.22 / 9.3.x < 9.3.18 / 9.4.x < 9.4.13 / 9.5.x < 9.5.8 / 9.6.x < 9.6.4 Multiple Vulnerabilities PostgreSQL 9.2.x < 9.2.24 / 9.3.x < 9.3.20 / 9.4.x < 9.4.15 / 9.5.x < 9.5.10 / 9.6.x < 9.6.6 / 10.x < 10.1 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de PostgresSQL que se ejecuta en el servidor se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a PostgreSQL versión 8.4.17 / 9.2.24 / 9.3.20 / 9.4.15 / 9.5.10 / 9.6.6 / 10.1 o posterior.
Dispositivos Afectados	10.1.4.206-fmorales.minedu.gov.co

	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities Apache 2.2.x < 2.2.23 Multiple Vulnerabilities Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities Apache 2.2.x < 2.2.25 Multiple Vulnerabilities Apache 2.2.x < 2.2.27 Multiple Vulnerabilities Apache 2.2.x < 2.2.28 Multiple Vulnerabilities Apache 2.2.x < 2.2.32 Multiple Vulnerabilities (httpoxy) Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS) Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass Apache 2.4.6 Remote DoS Apache 2.4.x < 2.4.10 Multiple Vulnerabilities Apache 2.4.x < 2.4.12 Multiple Vulnerabilities Apache 2.4.x < 2.4.16 Multiple Vulnerabilities Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy) Apache 2.4.x < 2.4.27 Multiple Vulnerabilities Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed) Apache 2.4.x < 2.4.33 Multiple Vulnerabilities Apache 2.4.x < 2.4.34 Multiple Vulnerabilities Apache 2.4.x < 2.4.35 DoS Apache 2.4.x < 2.4.38 Multiple Vulnerabilities Apache 2.4.x < 2.4.4 Multiple XSS Vulnerabilities Apache 2.4.x < 2.4.41 Multiple Vulnerabilities Apache 2.4.x < 2.4.42 Multiple Vulnerabilities Apache 2.4.x < 2.4.8 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El servidor web puede verse afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache versión 2.2.49 o posterior.
Dispositivos Afectados	10.1.100.30-MEN314492, 10.1.110.92-MEN317763, 10.1.120.199-MEN321040, 10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.5.103-MEN317763

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	Eliminar la página de índice predeterminada.
Dispositivos Afectados	10.1.120.199-MEN321040

Vulnerabilidad	Apache HTTP Server httpOnly Cookie Information Disclosure
Riesgo	Medio
Descripción	La versión de Apache HTTP Server que se ejecuta 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 (por ejemplo, secuencias de comandos entre sitios), podría resultar en el compromiso de las cookies httpOnly.
Solución	Actualice a la versión de Apache 2.0.65 / 2.2.22 o posterior.
Dispositivos Afectados	10.1.120.63-MEN317490, 10.1.150.60-MEN321032

Vulnerabilidad	Apache ServerTokens Information Disclosure

Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el host 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'
Dispositivos Afectados	10.1.100.30-MEN314492, 10.1.110.92-MEN317763, 10.1.120.199-MEN321040, 10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.5.103-MEN317763

Vulnerabilidad (x15)	Apache Tomcat < 6.0.32 / 7.0.8 NIO Connector DoS Apache Tomcat 6.0 < 6.0.28 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 Disclosure Apache Tomcat 6.0.x < 6.0.24 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.30 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.33 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.36 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.37 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.39 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.40 Multiple Vulnerabilities Apache Tomcat 6.0.x < 6.0.42 Handling Request Smuggling DoS Apache Tomcat 6.0.x < 6.0.45 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.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure Apache Tomcat 6.x < 6.0.30 / 7.x < 7.0.5 Multiple XSS
Riesgo	Medio
Descripción	El servidor Apache Tomcat puede verse afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache Tomcat versión 6.0.53/7.0.77/8.0.41/8.5.9/9.0.0.M15 o posterior.
Dispositivos Afectados	10.1.120.85-MEN317485

Vulnerabilidad (x15)	Apache Tomcat Default Files
Riesgo	Medio
Descripción	La página de error predeterminada, los JSP de ejemplo y/o los servlets de ejemplo están 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.
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.
Dispositivos Afectados	10.1.120.85-MEN317485

Vulnerabilidad (x15)	Apache Tomcat WAR Deployment Multiple Vulnerabilities
Riesgo	Medio
Descripción	Según la versión detectada, se está ejecutando una versión de Apache Tomcat que se ve afectada por múltiples vulnerabilidades: - Al implementar archivos WAR, los archivos WAR no se verifican en busca de intentos de cruce de directorios que podrían permitir que un atacante cree contenido arbitrario fuera de la raíz web. (CVE-2009-2693) - De forma predeterminada, Tomcat implementa automáticamente cualquier directorio ubicado en la base de aplicaciones de un host. Esto podría llevar a que los archivos que normalmente están protegidos por una o más restricciones de seguridad se implementen sin esas restricciones de seguridad. (CVE-2009-2901)

	- Al implementar archivos WAR, los nombres de los archivos WAR no se verifican en busca de intentos de cruce de directorios que podrían permitir que un atacante provoque la eliminación del contenido actual del directorio de trabajo del host. (CVE-2009-2902).
Solución	Actualice a Tomcat versión 6.0.24 / 5.5.29 o posterior.
Dispositivos Afectados	10.1.120.85-MEN317485

Vulnerabilidad (x15)	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	Deshabilitar tokens de servidor. Revise los archivos y reemplácelos o elimínelos según sea necesario.
Dispositivos Afectados	10.1.115.21, 10.1.120.126-MEN321039, 10.1.155.23

Vulnerabilidad	HTTP TRACE / TRACK Methods Allowedult nginx HTTP Server Settings
Riesgo	Medio
Descripción	El host admite los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
Solución	Deshabilite estos métodos HTTP.
Dispositivos Afectados	10.1.100.30-MEN314492, 10.1.110.92-MEN317763, 10.1.120.199-MEN321040, 10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.5.103-MEN317763

Vulnerabilidad (x5)	JQuery < 1.9.0 XSS JQuery < 3.0.0 XSS JQuery < 3.4.0 Object Prototype Pollution Vulnerability JQuery 1.2 < 3.5.0 Multiple XSS JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	El host se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Dispositivos Afectados	10.1.110.92-MEN317763, 10.1.5.103-MEN317763, 10.1.100.30-MEN314492, 10.1.120.47-MEN321904

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web utiliza la página de índice de IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Dispositivos Afectados	10.1.120.63-MEN317490

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 de 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 el 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 - Seleccione la configuración 'Permitir conexiones solo desde computadoras que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.110.64-MEN3178000, 10.1.115.29-MEN319243, 10.1.120.103-MEN317458, 10.1.120.29-MEN317482, 10.1.120.44-MEN314589, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.85-MEN317485

Vulnerabilidad	MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure (824105) (uncredentialed check)
Riesgo	Medio
Descripción	El host remoto está ejecutando una versión del servicio de nombres NetBT que sufre un problema de divulgación de memoria. Un atacante puede enviar un paquete especial al servicio de nombres NetBT remoto y la respuesta contendrá datos arbitrarios aleatorios de la memoria del host. Estos datos arbitrarios pueden ser un fragmento de la página web que está viendo el usuario remoto o algo más serio como una contraseña. Un atacante puede usar esta falla para "sondear" continuamente el contenido de la memoria del host remoto y podría obtener información confidencial.
Solución	Microsoft ha lanzado parches para Windows NT, 2000, XP y 2003.
Dispositivos Afectados	10.1.5.75

Vulnerabilidad	MS14-044: Vulnerability in SQL Server Could Allow Elevation of Privilege (2984340) (uncredentialed check)
Riesgo	Medio
Descripción	El host remoto tiene instalada una versión de Microsoft SQL Server. Esta versión de SQL Server está potencialmente afectada por múltiples vulnerabilidades: - Existe una vulnerabilidad de secuencias de comandos entre sitios en SQL Master Data Services. (CVE-2014-1820) - Existe una vulnerabilidad de denegación de servicio en SQL Server. (CVE-2014-4061)
Solución	Microsoft ha lanzado un conjunto de parches para SQL Server 2008, 2008 R2, 2012 y 2014.
Dispositivos Afectados	10.1.150.130-MEN317457

Vulnerabilidad	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Riesgo	Medio
Descripción	El host 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 man-in-the-middle 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.
Dispositivos Afectados	10.1.100.22-MEN311015.

Vulnerabilidad (x3)	nginx < 1.17.7 Information Disclosure nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE

	nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El host se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a nginx 1.20.1 o posterior.
Dispositivos Afectados	10.1.155.23

Vulnerabilidad	OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities OpenSSL 1.1.0 < 1.1.0k Vulnerability OpenSSL 1.1.0 < 1.1.0l Multiple Vulnerabilities
Riesgo	Medio
Descripción	Un servicio que se ejecuta en el host se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche del proveedor o actualice a OpenSSL versión 1.1.0L o posterior.
Dispositivos Afectados	10.1.100.30-MEN314492

Vulnerabilidad (x2)	Oracle Application Express (Apex) CVE-2011-3525 Oracle Application Express (Apex) CVE-2012-1708
Riesgo	Medio
Descripción	El host remoto ejecuta una versión vulnerable de Oracle Apex.
Solución	Actualice Application Express al menos a la versión 4.1.1.
Dispositivos Afectados	10.1.110.92-MEN317763

Vulnerabilidad (x42)	PHP < 5.2.10 Multiple Vulnerabilities PHP < 5.2.12 Multiple Vulnerabilities PHP < 5.2.9 Multiple Vulnerabilities PHP < 5.3.11 Multiple Vulnerabilities PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities PHP < 7.3.24 Multiple Vulnerabilities PHP < 7.3.28 Email Header Injection PHP 5.2 < 5.2.15 Multiple Vulnerabilities PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS PHP 5.2.x filter_globals Subsequence Request Parsing Remote Code Execution PHP 5.6.x < 5.6.14 Multiple Vulnerabilities PHP 5.6.x < 5.6.28 Multiple Vulnerabilities PHP 5.6.x < 5.6.33 Multiple Vulnerabilities PHP 5.6.x < 5.6.36 Multiple Vulnerabilities PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability PHP 7.0.x < 7.0.30 Multiple Vulnerabilities PHP 7.0.x < 7.0.32 Transfer-Encoding Parameter XSS Vulnerability PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Mulitiple Vulnerabilities PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability PHP 7.2.x < 7.2.17 Multiple vulnerabilities. PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability. PHP 7.2.x < 7.2.19 Multiple Vulnerabilities. PHP 7.2.x < 7.2.21 Multiple Vulnerabilities. PHP 7.2.x < 7.2.26 Multiple Vulnerabilities

	PHP 7.2.x < 7.2.27 / PHP 7.3.x < 7.3.14 / 7.4.x < 7.4.2 Multiple Vulnerabilities PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities PHP 7.2.x < 7.2.29 Multiple Vulnerabilities PHP 7.2.x < 7.2.30 Multiple Vulnerabilities PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS) PHP 7.2.x < 7.2.32 / 7.3.x < 7.3.20 / 7.4.x < 7.4.8 Information Disclosure PHP 7.3.x < 7.3.16 Multiple Vulnerabilities PHP 7.3.x < 7.3.17 Out of Bounds Read Vulnerability 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 7.3.x < 7.3.31 Arbitrary File Write PHP 7.3.x < 7.3.32 PHP 7.3.x < 7.3.33 PHP PHP_RSHUTDOWN_FUNCTION Security Bypass PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de PHP que se ejecuta en el servidor web se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a la versión de PHP 7.3.33/7.4.15/8.0.2 o posterior.
Dispositivos Afectados	10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.100.30-MEN314492, 10.1.110.92-MEN317763, 10.1.5.103-MEN317763

Vulnerabilidad (x9)	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 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 File Deletion 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 < 9.1.9 / 9.2 < 9.2.4 Denial of Service 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 9.2.x < 9.2.21 / 9.3.x < 9.3.17 / 9.4.x < 9.4.12 / 9.5.x < 9.5.7 / 9.6.x < 9.6.3 Multiple Vulnerabilities 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
Riesgo	Medio
Descripción	El servidor de la base de datos remota se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a PostgreSQL 8.3.23/8.4.20/9.0.16/9.1.23/9.2.21/9.3.23/9.4.18/9.5.13/9.6.9/10.3 o posterior.
Dispositivos Afectados	10.1.4.206-fmorales.minedu.gov.co

Vulnerabilidad (x5)	Samba 4.3.x < 4.3.13 / 4.4.x < 4.4.8 / 4.5.x < 4.5.3 Multiple Vulnerabilities Samba 4.x < 4.8.12 / 4.9.x < 4.9.8 / 4.10.x < 4.10.3 Man in the Middle Vulnerability (CVE-2018-16860) Samba 4.x < 4.9.15 / 4.10.x < 4.10.10 AD DC LDAP Server Denial of Service (CVE-2019-14847) Samba 4.x < 4.9.17 / 4.10.x < 4.10.11 / 4.11.x < 4.11.3 Multiple Vulnerabilities Samba 4.x < 4.9.18 / 4.10.x < 4.10.12 / 4.11.x < 4.11.5 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El servidor Samba remoto se ve potencialmente afectado por múltiples vulnerabilidades.
Solución	Actualice a Samba 4.9.18 / 4.10.12 / 4.11.5 o posterior.
Dispositivos Afectados	10.1.150.147

Vulnerabilidad (x5)	Samba 4.3.x < 4.3.13 / 4.4.x < 4.4.8 / 4.5.x < 4.5.3 Multiple Vulnerabilities Samba 4.x < 4.8.12 / 4.9.x < 4.9.8 / 4.10.x < 4.10.3 Man in the Middle Vulnerability (CVE-2018-16860) Samba 4.x < 4.9.15 / 4.10.x < 4.10.10 AD DC LDAP Server Denial of Service (CVE-2019-14847)

	Samba 4.x < 4.9.17 / 4.10.x < 4.10.11 / 4.11.x < 4.11.3 Multiple Vulnerabilities Samba 4.x < 4.9.18 / 4.10.x < 4.10.12 / 4.11.x < 4.11.5 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El servidor Samba remoto se ve potencialmente afectado por múltiples vulnerabilidades.
Solución	Actualice a Samba 4.9.18 / 4.10.12 / 4.11.5 o posterior.
Dispositivos Afectados	10.1.150.147

Vulnerabilidad	Security Updates for Microsoft SQL Server (May 2019)
Riesgo	Medio
Descripción	Falta una actualización de seguridad en la instalación de Microsoft SQL Server en el host remoto. 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 aprovechara 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
Dispositivos Afectados	10.1.140.48-MEN321104, 10.1.140.83-MEN319368, 10.1.150.130-MEN317457

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: - Existe una vulnerabilidad de ejecución remota de código en Microsoft SQL Server cuando maneja incorrectamente el procesamiento de funciones internas. Un atacante que aproveche 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
Dispositivos Afectados	10.1.140.48-MEN321104, 10.1.140.83-MEN319368, 10.1.150.130-MEN317457

Vulnerabilidad	SMB Signing not required
Riesgo	Medio
Descripción	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB.
Solución	Haga 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'.

Dispositivos Afectados	10.1.100.22-MEN311015, 10.1.100.23-MEN316938, 10.1.100.27-MEN317257, 10.1.100.28-MEN314502, 10.1.100.29-MEN317263, 10.1.100.30-MEN314492, 10.1.100.32-MEN314546, 10.1.100.33-MEN311994, 10.1.100.38-MEN314668, 10.1.100.39-MEN311831, 10.1.100.41-MEN321581, 10.1.100.42-MEN314142, 10.1.100.43-MEN315305, 10.1.100.44-MEN315262, 10.1.100.53-MEN306796, 10.1.105.22-MEN314695, 10.1.110.107-MEN320202, 10.1.110.162-MEN314536, 10.1.110.199-UAC_CARTELERA_PISO_1, 10.1.110.222-MEN314086, 10.1.110.25-Men314797, 10.1.110.25-MEN317982, 10.1.110.26-Men314797, 10.1.110.27-MEN317813, 10.1.110.30-MEN307888, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.44-MEN317489, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.57-MEN314526, 10.1.110.58-MEN315302, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.66-MEN311989, 10.1.110.68-MEN314573, 10.1.110.69-MEN317804, 10.1.110.72-MEN317921, 10.1.110.79-MEN314060, 10.1.110.80-Cartelerasuac3, 10.1.110.81-Cartelerasuac1, 10.1.110.89-MEN314607, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.22-MEN314678, 10.1.115.24-MEN314468, 10.1.115.25-MEN317943, 10.1.115.28-MEN319378, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.34-MEN314062, 10.1.115.35-MEN317970, 10.1.115.36-MEN314656, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.41-MEN320805, 10.1.115.42-MEN323045, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.54-MEN311813, 10.1.115.57-MEN321115, 10.1.115.63-MEN320752, 10.1.115.64-MEN322458, 10.1.115.65-MEN320807, 10.1.115.74-MEN315283, 10.1.115.75-MEN317950, 10.1.115.86-MEN320758, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.95-MEN320796, 10.1.115.96-MEN314514, 10.1.120.100-CJ11871, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.104-Cartelera_Recepcion_1, 10.1.120.110-MEN321070, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.120-MEN310988, 10.1.120.122-MEN321124, 10.1.120.125-CARTELERA_RECEPCION_2_PARQUEADERO, 10.1.120.126-MEN321039, 10.1.120.129-Cartelera_Tecnologia, 10.1.120.133-MEN317919, 10.1.120.137-CARTELERA_TALENTO_HUMANO_PISO_2, 10.1.120.138-MEN314064, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.174-MEN320848, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.49-DESKTOP-8Q331HK, 10.1.120.51-MEN319358, 10.1.120.52-MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.70-MEN320732, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.155-MEN320751, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.52-MEN317930, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.68-MEN314545, 10.1.125.69-MEN319377, 10.1.125.78-MEN319337, 10.1.125.82-MEN319350, 10.1.125.84-CARTELERA_FINANCIERA, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.103-MEN317993, 10.1.130.113-CARTELERA-ACCESO_PISO-3, 10.1.130.118-MEN314621, 10.1.130.139-MEN314601, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.26-MEN319224, 10.1.130.31-MEN315267, 10.1.130.32-MEN314652, 10.1.130.33-MEN320742, 10.1.130.34-MEN314701, 10.1.130.35-MEN320753, 10.1.130.37-MEN317239, 10.1.130.38-MEN317864, 10.1.130.39-MEN317932, 10.1.130.41-MEN317808, 10.1.130.54-MEN319311, 10.1.130.55-MEN314506, 10.1.130.58-MEN317899, 10.1.130.59-MEN321033, 10.1.130.60-MEN319404, 10.1.130.64-MEN317862, 10.1.130.66-MEN315260, 10.1.130.77-MEN317965, 10.1.130.83-MEN317858, 10.1.130.85-CARTELERA_FORTALECIMIENTO_PISO_3, 10.1.135.120-MEN317827, 10.1.135.23-MEN317985, 10.1.135.29-MEN321112, 10.1.135.30-MEN321099, 10.1.135.36-MEN319277, 10.1.135.40-MEN319192, 10.1.135.57-MEN319194, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.121-MEN319394, 10.1.140.125-MEN319382, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.249-men319391, 10.1.140.25-CARTELERA_PRIMERA_INFANCIA_P4, 10.1.140.30-

	MEN317306, 10.1.140.43-MEN315303, 10.1.140.47-MEN319353, 10.1.140.48-MEN321104, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.62-MEN317494, 10.1.140.65-MEN314686, 10.1.140.66-MEN321899, 10.1.140.67-MEN319221, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.123-MEN317779, 10.1.145.125-MEN317293, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.30-MEN321961, 10.1.145.32-MEN320840, 10.1.145.38-men314548, 10.1.145.44-cARTELERA_FOMENTO, 10.1.145.48-MEN320795, 10.1.145.56-MEN317905, 10.1.145.92-MEN320839, 10.1.150.100-MEN320801, 10.1.150.104-MEN319324, 10.1.150.108-MEN319406, 10.1.150.109-MEN314529, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.114-MEN317302, 10.1.150.115-MEN319434, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.125-DESKTOP-4PKJT1N, 10.1.150.130-MEN317457, 10.1.150.141-MEN319251, 10.1.150.147, 10.1.150.149-MEN317939, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.34-MEN314633, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-MEN319316, 10.1.150.73-MEN314563, 10.1.150.78-MEN319318, 10.1.150.79-MEN317781, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.92-MEN319419, 10.1.150.94-men314588, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.24-MEN314541, 10.1.155.27-MEN315297, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.38-MEN319235, 10.1.155.39-MEN319417, 10.1.155.40-MEN317840, 10.1.155.41-MEN315236, 10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.46-MEN320780, 10.1.155.48-MEN321121, 10.1.155.51-MEN320809, 10.1.155.52-MEN319265, 10.1.155.54-MEN317842, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.111-LAPTOP-E7LHDMH6, 10.1.4.125-MEN320866, 10.1.4.133-MEN319650, 10.1.4.139-MEN319650, 10.1.4.141-MEN319438, 10.1.4.145-MEN319517, 10.1.4.148-CJ12189, 10.1.4.152-MEN317550, 10.1.4.152-MEN320845, 10.1.4.154-MEN321945, 10.1.4.156-CJ12189, 10.1.4.160-MEN321946, 10.1.4.162-MEN320752, 10.1.4.166-10891CJ, 10.1.4.169-DESKTOP-K7O8R0L, 10.1.4.177-MEN319601, 10.1.4.178-MEN321971, 10.1.4.189-MEN317601, 10.1.4.192-MEN319641, 10.1.4.206-fmorales, 10.1.4.210-MEN320760, 10.1.4.214-MEN321977, 10.1.4.219-MEN317510, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.252-MEN317922, 10.1.4.255-MEN321961, 10.1.4.37-MEN319513, 10.1.4.47-MEN321945, 10.1.4.50-MEN319513, 10.1.4.56-MEN320849, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.4.85-MEN320859, 10.1.4.92-MEN319701, 10.1.5.0-DESKTOP-K7O8R0L, 10.1.5.0-DESKTOP-V8JKO2L, 10.1.5.103-MEN317763, 10.1.5.105, 10.1.5.13-CJ10315, 10.1.5.132-MEN321132, 10.1.5.140-MEN321899, 10.1.5.145-MEN319567, 10.1.5.166-MEN321086, 10.1.5.23-MEN320797, 10.1.5.31-MEN321122, 10.1.5.44-MEN317510, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.50-MEN317354, 10.1.5.60-MEN321946, 10.1.5.69-MEN320762, 10.1.5.79-MEN321115, 10.1.5.8-12227CJ, 10.1.5.84-MEN321128, 10.1.5.89, 10.1.5.9, 10.1.5.93-DESKTOP-V8JKO2L, 10.1.5.95-12227CJ, 10.1.6.7-MEN320794

Vulnerabilidad	SSH Weak Algorithms Supported
Riesgo	Medio
Descripción	Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo 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.
Dispositivos Afectados	10.1.130.58-MEN317899, 10.1.150.130-MEN317457, 10.1.150.81-MEN317456

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloques 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 man-in-the-middle que tenga suficientes recursos puede explotar esta vulnerabilidad, a través de un ataque 'birthday', para detectar una colisión que filtre el XOR entre el texto secreto

	y un texto sin formato conocido, lo que permite la divulgación del texto secreto como cookies HTTPS seguras, y que posiblemente resulte en el secuestro de una sesión autenticada. Las pruebas de concepto han demostrado que los atacantes pueden recuperar las cookies de autenticación de una sesión HTTPS en tan solo 30 horas. Tenga en cuenta que la capacidad de enviar una gran cantidad de solicitudes a través de la misma conexión TLS entre el cliente y el servidor es un requisito importante para llevar a cabo este ataque. Si se limitara el número de solicitudes permitidas para una única conexión, se mitigaría la vulnerabilidad.
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 pueden procesarse a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.27-MEN317257, 10.1.100.30-MEN314492, 10.1.100.41-MEN321581, 10.1.110.107-MEN320202, 10.1.110.27-MEN317813, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.46-MEN322104, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.58-MEN315302, 10.1.110.61-Men317455, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.69-MEN317804, 10.1.110.79-MEN314060, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.25-MEN317943, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.57-MEN321115, 10.1.115.63-MEN320752, 10.1.115.65-MEN320807, 10.1.115.75-MEN317950, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.96-MEN314514, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.122-MEN321124, 10.1.120.126-MEN321039, 10.1.120.133-MEN317919, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.47-MEN321904, 10.1.120.51-MEN319358, 10.1.120.52-MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.152-MEN321158, 10.1.125.155-MEN320751, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.49-MEN321868, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.78-MEN319337, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.118-MEN314621, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.31-MEN315267, 10.1.130.33-MEN320742, 10.1.130.35-MEN320753, 10.1.130.39-MEN317932, 10.1.130.54-MEN319311, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.135.29-MEN321112, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.30-MEN317306, 10.1.140.48-MEN321104, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.38-men314548, 10.1.145.48-MEN320795, 10.1.145.92-MEN320839, 10.1.150.104-MEN319324, 10.1.150.105-MEN321901, 10.1.150.108-MEN319406, 10.1.150.110-MEN321149, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.113-MEN321146, 10.1.150.114-MEN317302, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.127-MEN321156, 10.1.150.130-MEN317457, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-

	MEN319316, 10.1.150.73-MEN314563, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.24-MEN314541, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.36-MEN321902, 10.1.155.38-MEN319235, 10.1.155.40-MEN317840, 10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.48-MEN321121, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.113-11301CJ, 10.1.4.141-MEN319438, 10.1.4.162-MEN320752, 10.1.4.210-MEN320760, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.37-MEN319513, 10.1.4.50-MEN319513, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.5.103-MEN317763, 10.1.5.132-MEN321132, 10.1.5.145-MEN319567, 10.1.5.28-MEN321912, 10.1.5.31-MEN321122, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.79-MEN321115, 10.1.5.9

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas distintas, en las que se puede romper la cadena de confianza, como se expone a continuación: - En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento de la exploración. Esto puede ocurrir cuando la exploración ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. - En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las firmas incorrectas se pueden corregir haciendo que el emisor vuelva a firmar el certificado que tiene la firma incorrecta. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del host. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.27-MEN317257, 10.1.100.30-MEN314492, 10.1.100.41-MEN321581, 10.1.110.107-MEN320202, 10.1.110.27-MEN317813, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.46-MEN322104, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.58-MEN315302, 10.1.110.59-MEN321910, 10.1.110.61-Men317455, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.69-MEN317804, 10.1.110.79-MEN314060, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.25-MEN317943, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.34-MEN314062, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.42-MEN323045, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.57-MEN321115, 10.1.115.59-MEN321889, 10.1.115.63-MEN320752, 10.1.115.65-MEN320807, 10.1.115.75-MEN317950, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.96-MEN314514, 10.1.120.100-CJ11871, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.122-MEN321124, 10.1.120.126-MEN321039, 10.1.120.133-MEN317919, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.174-MEN320848, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.47-MEN321904, 10.1.120.51-MEN319358, 10.1.120.52-

	MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.152-MEN321158, 10.1.125.155-MEN320751, 10.1.125.21-MEN321414, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.49-MEN321868, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.68-MEN314545, 10.1.125.78-MEN319337, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.118-MEN314621, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.31-MEN315267, 10.1.130.33-MEN320742, 10.1.130.35-MEN320753, 10.1.130.39-MEN317932, 10.1.130.54-MEN319311, 10.1.130.58-MEN317899, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.66-MEN315260, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.135.26-MEN321152, 10.1.135.29-MEN321112, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.133-MEN314484, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.30-MEN317306, 10.1.140.41-MEN315295, 10.1.140.43-MEN315303, 10.1.140.48-MEN321104, 10.1.140.50-MEN319276, 10.1.140.53-MEN314619, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.31-MEN320790, 10.1.145.38-men314548, 10.1.145.48-MEN320795, 10.1.145.92-MEN320839, 10.1.145.93-MEN317258, 10.1.150.104-MEN319324, 10.1.150.105-MEN321901, 10.1.150.108-MEN319406, 10.1.150.110-MEN321149, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.113-MEN321146, 10.1.150.114-MEN317302, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.127-MEN321156, 10.1.150.130-MEN317457, 10.1.150.147, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-MEN319316, 10.1.150.73-MEN314563, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.23, 10.1.155.24-MEN314541, 10.1.155.27-MEN315297, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.36-MEN321902, 10.1.155.37-MEN317958, 10.1.155.38-MEN319235, 10.1.155.40-MEN317840, 10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.48-MEN321121, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.113-11301CJ, 10.1.4.119-MEN317345, 10.1.4.133-MEN321941, 10.1.4.141-MEN319438, 10.1.4.148-CJ12189, 10.1.4.156-CJ12189, 10.1.4.162-MEN320752, 10.1.4.210-MEN320760, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.37-MEN319513, 10.1.4.50-MEN319513, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.5.103-MEN317763, 10.1.5.13-CJ10315, 10.1.5.132-MEN321132, 10.1.5.145-MEN319567, 10.1.5.28-MEN321912, 10.1.5.31-MEN321122, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.50-MEN317354, 10.1.5.79-MEN321115, 10.1.5.84-MEN321128, 10.1.5.9

Vulnerabilidad	SSL Certificate Expiry
Riesgo	Medio
Descripción	Este complemento comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados de SSL e informa si alguno ya ha caducado.
Solución	Compre o genere un nuevo certificado SSL para reemplazar el existente.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.30-MEN314492

Vulnerabilidad	SSL Certificate Signed Using Weak Hashing Algorithm
Riesgo	Medio

Descripción	El host utiliza una cadena de certificados SSL que se ha firmado con un algoritmo 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 explotar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado. Tenga en cuenta que este complemento informa que todas las cadenas de certificados SSL firmadas con SHA-1 que vencen después del 1 de enero de 2017 son vulnerables. Esto está de acuerdo con la extinción gradual de Google del algoritmo hash criptográfico SHA-1.
Solución	Póngase en contacto con la autoridad certificadora para que le vuelvan a emitir el certificado SSL.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.30-MEN314492, 10.1.115.29-MEN319243, 10.1.120.103-MEN317458, 10.1.120.29-MEN317482, 10.1.120.44-MEN314589, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.85-MEN317485, 10.1.130.58-MEN317899, 10.1.150.130-MEN317457, 10.1.150.147

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.
Dispositivos Afectados	10.1.100.30-MEN314492, 10.1.115.43-men314054, 10.1.120.63-MEN317490, 10.1.120.85-MEN317485, 10.1.140.48-MEN321104, 10.1.140.83-MEN319368, 10.1.145.38-men314548, 10.1.150.130-MEN317457, 10.1.150.147

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. Se considera de fuerza media cualquier cifrado que use longitudes de clave de al menos 64 bits y menos de 112 bits, o que use la suite de encriptación 3DES. Tenga en cuenta que es considerablemente más fácil eludir el cifrado de nivel medio si el atacante está en la misma red física.
Solución	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.27-MEN317257, 10.1.100.41-MEN321581, 10.1.110.107-MEN320202, 10.1.110.27-MEN317813, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.46-MEN322104, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.58-MEN315302, 10.1.110.61-Men317455, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.69-MEN317804, 10.1.110.79-MEN314060, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.25-MEN317943, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.57-MEN321115, 10.1.115.63-MEN320752, 10.1.115.65-MEN320807, 10.1.115.75-MEN317950, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.96-MEN314514, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.122-MEN321124, 10.1.120.126-MEN321039, 10.1.120.133-MEN317919, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.47-MEN321904, 10.1.120.51-MEN319358, 10.1.120.52-MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.152-

	MEN321158, 10.1.125.155-MEN320751, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.49-MEN321868, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.78-MEN319337, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.118-MEN314621, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.31-MEN315267, 10.1.130.33-MEN320742, 10.1.130.35-MEN320753, 10.1.130.39-MEN317932, 10.1.130.54-MEN319311, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.135.29-MEN321112, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.30-MEN317306, 10.1.140.48-MEN321104, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.38-men314548, 10.1.145.48-MEN320795, 10.1.145.92-MEN320839, 10.1.150.104-MEN319324, 10.1.150.105-MEN321901, 10.1.150.108-MEN319406, 10.1.150.110-MEN321149, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.113-MEN321146, 10.1.150.114-MEN317302, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.127-MEN321156, 10.1.150.130-MEN317457, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-MEN319316, 10.1.150.73-MEN314563, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.24-MEN314541, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.36-MEN321902, 10.1.155.38-MEN319235, 10.1.155.40-MEN317840, 10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.48-MEN321121, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.113-11301CJ, 10.1.4.141-MEN319438, 10.1.4.162-MEN320752, 10.1.4.210-MEN320760, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.37-MEN319513, 10.1.4.50-MEN319513, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.5.103-MEN317763, 10.1.5.132-MEN321132, 10.1.5.145-MEN319567, 10.1.5.28-MEN321912, 10.1.5.31-MEN321122, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.79-MEN321115, 10.1.5.9

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 pseudoaleatorios, por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad. Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (decenas de millones) textos cifrados, el atacante puede obtener el texto sin formato.
Solución	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.110.92-MEN317763, 10.1.115.29-MEN319243, 10.1.115.46-MEN319298, 10.1.120.103-MEN317458, 10.1.120.29-MEN317482, 10.1.120.44-MEN314589, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.68-MEN317795, 10.1.120.71-MEN317978, 10.1.120.85-MEN317485, 10.1.125.32-MEN317971, 10.1.125.34-MEN317988, 10.1.130.24-MEN319304, 10.1.130.54-MEN319311, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.150.147, 10.1.150.67-men314588, 10.1.4.222-MEN317850, 10.1.5.103-MEN317763

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque de man-in-the-middle contra el host remoto. Tenga en cuenta que este complemento no comprueba las

	cadenas de certificados que terminan en un certificado que no está autofirmado, pero que está firmado por una autoridad de certificación no reconocida.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.27-MEN317257, 10.1.100.30-MEN314492, 10.1.100.41-MEN321581, 10.1.110.107-MEN320202, 10.1.110.27-MEN317813, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.46-MEN322104, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.58-MEN315302, 10.1.110.59-MEN321910, 10.1.110.61-Men317455, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.69-MEN317804, 10.1.110.79-MEN314060, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.25-MEN317943, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.34-MEN314062, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.42-MEN323045, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.57-MEN321115, 10.1.115.59-MEN321889, 10.1.115.63-MEN320752, 10.1.115.65-MEN320807, 10.1.115.75-MEN317950, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.96-MEN314514, 10.1.120.100-CJ11871, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.122-MEN321124, 10.1.120.126-MEN321039, 10.1.120.133-MEN317919, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.174-MEN320848, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.47-MEN321904, 10.1.120.51-MEN319358, 10.1.120.52-MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.152-MEN321158, 10.1.125.155-MEN320751, 10.1.125.21-MEN321414, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.49-MEN321868, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.68-MEN314545, 10.1.125.78-MEN319337, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.118-MEN314621, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.31-MEN315267, 10.1.130.33-MEN320742, 10.1.130.35-MEN320753, 10.1.130.39-MEN317932, 10.1.130.54-MEN319311, 10.1.130.58-MEN317899, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.66-MEN315260, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.135.26-MEN321152, 10.1.135.29-MEN321112, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.133-MEN314484, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.30-MEN317306, 10.1.140.41-MEN315295, 10.1.140.43-MEN315303, 10.1.140.48-MEN321104, 10.1.140.50-MEN319276, 10.1.140.53-MEN314619, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.31-MEN320790, 10.1.145.38-men314548, 10.1.145.48-MEN320795, 10.1.145.92-MEN320839, 10.1.145.93-MEN317258, 10.1.150.104-MEN319324, 10.1.150.105-MEN321901, 10.1.150.108-MEN319406, 10.1.150.110-MEN321149, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.113-MEN321146, 10.1.150.114-MEN317302, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.127-MEN321156, 10.1.150.130-MEN317457, 10.1.150.147, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-MEN319316, 10.1.150.73-MEN314563, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.24-MEN314541, 10.1.155.27-MEN315297, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.36-MEN321902, 10.1.155.37-MEN317958, 10.1.155.38-MEN319235, 10.1.155.40-MEN317840,

	10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.48-MEN321121, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.113-11301CJ, 10.1.4.119-MEN317345, 10.1.4.133-MEN321941, 10.1.4.141-MEN319438, 10.1.4.148-CJ12189, 10.1.4.156-CJ12189, 10.1.4.162-MEN320752, 10.1.4.210-MEN320760, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.37-MEN319513, 10.1.4.50-MEN319513, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.5.103-MEN317763, 10.1.5.13-CJ10315, 10.1.5.132-MEN321132, 10.1.5.145-MEN319567, 10.1.5.28-MEN321912, 10.1.5.31-MEN321122, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.50-MEN317354, 10.1.5.79-MEN321115, 10.1.5.84-MEN321128, 10.1.5.9

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 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 bloques 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 admitan SSLv3, una conexión se puede "revertir" a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o una versión más reciente. El mecanismo TLS Fallback SCSV evita los ataques de "reversión de versión" 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 inmediatamente deben habilitar este mecanismo. Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación SSL en particular. Deshabilitar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.
Solución	Deshabilitar SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda deshabilitar SSLv3.
Dispositivos Afectados	10.1.120.85-MEN317485

Vulnerabilidad	TCP/IP SYN+FIN Packet Filtering Weakness
Riesgo	Medio
Descripción	El host no descarta los paquetes TCP SYN que tienen el indicador FIN establecido. Dependiendo del tipo de firewall que esté utilizando, un atacante puede usar esta falla para eludir sus reglas.
Solución	Póngase en contacto con su proveedor para obtener un parche.
Dispositivos Afectados	10.1.110.45

Vulnerabilidad	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Riesgo	Medio
Descripción	Los Servicios de Terminal Server no están configurados para utilizar únicamente la Autenticación de nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para realizar una fuerte autenticación de servidor a través de TLS/SSL o mecanismos Kerberos, que protegen contra ataques de man-in-the-middle. Además de mejorar la autenticación, NLA también ayuda a proteger la computadora remota de usuarios y software maliciosos al completar la autenticación del usuario antes de que se establezca una conexión RDP completa.
Solución	Habilite la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto generalmente se hace en la pestaña 'Remoto' de la configuración de 'Sistema' en Windows.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.110.52-MEN314631, 10.1.110.64-MEN3178000, 10.1.115.29-MEN319243, 10.1.115.43-men314054, 10.1.120.103-MEN317458, 10.1.120.140-MEN315294, 10.1.120.206-MEN320747,

	10.1.120.21-MEN319416, 10.1.120.237-MEN319299, 10.1.120.29-MEN317482, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.71-MEN317978, 10.1.120.74-MEN319213, 10.1.120.85-MEN317485, 10.1.120.92-MEN317486, 10.1.125.34-MEN317988, 10.1.125.78-MEN319337, 10.1.130.101-MEN321033, 10.1.130.39-MEN317932, 10.1.135.120-MEN317827, 10.1.140.91-MEN317854, 10.1.145.129-MEN320778, 10.1.145.29-MEN319360, 10.1.155.30-MEN315287, 10.1.155.36-MEN321902

Vulnerabilidad	Terminal Services Encryption Level is Medium or Low
Riesgo	Medio
Descripción	El servicio de Terminal Services no está configurado para usar criptografía fuerte. El uso de criptografía débil con este servicio puede permitir que un atacante espíe las comunicaciones más fácilmente y obtenga capturas de pantalla y/o pulsaciones de teclas.
Solución	Cambie el nivel de cifrado RDP a uno de: 3. alto 4. Cumplimiento con FIPS
Dispositivos Afectados	10.1.110.64-MEN3178000, 10.1.115.29-MEN319243, 10.1.120.103-MEN317458, 10.1.120.29-MEN317482, 10.1.120.44-MEN314589, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.85-MEN317485

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El host acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios 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 para estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los endpoints que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.100.27-MEN317257, 10.1.100.30-MEN314492, 10.1.100.41-MEN321581, 10.1.110.107-MEN320202, 10.1.110.27-MEN317813, 10.1.110.31-MEN314471, 10.1.110.42-MEN317483, 10.1.110.46-MEN322104, 10.1.110.48-MEN317807, 10.1.110.52-MEN314631, 10.1.110.55-PORTAFIRMAS, 10.1.110.58-MEN315302, 10.1.110.61-Men317455, 10.1.110.64-MEN3178000, 10.1.110.65-Men319369, 10.1.110.69-MEN317804, 10.1.110.79-MEN314060, 10.1.110.92-MEN317763, 10.1.110.97-MEN314475, 10.1.115.117-MEN320737, 10.1.115.123-MEN321147, 10.1.115.125-MEN321139, 10.1.115.25-MEN317943, 10.1.115.29-MEN319243, 10.1.115.33-MEN321089, 10.1.115.38-MEN321708, 10.1.115.39-MEN315263, 10.1.115.43-men314054, 10.1.115.46-MEN319298, 10.1.115.47-MEN321914, 10.1.115.50-MEN320783, 10.1.115.57-MEN321115, 10.1.115.63-MEN320752, 10.1.115.65-MEN320807, 10.1.115.75-MEN317950, 10.1.115.91-MEN320735, 10.1.115.93-MEN320726, 10.1.115.96-MEN314514, 10.1.120.102-MEN321081, 10.1.120.103-MEN317458, 10.1.120.114-MEN317826, 10.1.120.117-Soportemda20, 10.1.120.122-MEN321124, 10.1.120.126-MEN321039, 10.1.120.133-MEN317919, 10.1.120.140-MEN315294, 10.1.120.142-MEN0321041, 10.1.120.143-MEN314618, 10.1.120.167-MEN320741, 10.1.120.175-MEN317487, 10.1.120.196-LAPTOP-A632S92Q, 10.1.120.199-MEN321040, 10.1.120.205-MEN317920, 10.1.120.206-MEN320747, 10.1.120.21-MEN319416, 10.1.120.214-MEN321087, 10.1.120.22-MEN314515, 10.1.120.235-MEN314592, 10.1.120.237-MEN319299, 10.1.120.238-MDABACKUPS, 10.1.120.251-O1APPBK01, 10.1.120.29-MEN317482, 10.1.120.31-CJ11722, 10.1.120.33-DESKTOP-330214, 10.1.120.36-MEN315265, 10.1.120.38-MEN317829, 10.1.120.39-MEN319339, 10.1.120.43-DESKTOP-carvajal, 10.1.120.44-MEN314589, 10.1.120.45-MEN315291, 10.1.120.46-MEN314670, 10.1.120.47-MEN321904, 10.1.120.51-MEN319358, 10.1.120.52-MEN317778, 10.1.120.54-MEN321038, 10.1.120.58-MEN317454, 10.1.120.62-MEN315240, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.67-MEN321890, 10.1.120.68-MEN317795, 10.1.120.69-MEN317992, 10.1.120.71-MEN317978, 10.1.120.73-Alejandro, 10.1.120.74-MEN319213, 10.1.120.79-MEN319407, 10.1.120.82-MEN320774, 10.1.120.84-MEN317951, 10.1.120.85-MEN317485, 10.1.120.86-MEN315239, 10.1.120.88-MEN319693, 10.1.120.92-MEN317486, 10.1.120.96-MEN319567, 10.1.125.123-MEN321906, 10.1.125.125-MEN319177, 10.1.125.136-ME317768, 10.1.125.152-MEN321158, 10.1.125.155-MEN320751, 10.1.125.22-MEN319344, 10.1.125.23-MEN321119, 10.1.125.26-MEN319260, 10.1.125.27-MEN319411, 10.1.125.32-

	MEN317971, 10.1.125.33-MEN317924, 10.1.125.34-MEN317988, 10.1.125.36-MEN314088, 10.1.125.39-MEN314520, 10.1.125.40-MEN321127, 10.1.125.45-MEN317983, 10.1.125.49-MEN321868, 10.1.125.59-MEN314602, 10.1.125.61-MEN319346, 10.1.125.78-MEN319337, 10.1.125.87-MEN321090, 10.1.125.92-MEN321108, 10.1.125.94-MEN314562, 10.1.125.96-MEN321092, 10.1.125.97-MEN314048, 10.1.130.100-MEN321034, 10.1.130.101-MEN321033, 10.1.130.118-MEN314621, 10.1.130.21-MEN317495, 10.1.130.24-MEN319304, 10.1.130.31-MEN315267, 10.1.130.33-MEN320742, 10.1.130.35-MEN320753, 10.1.130.39-MEN317932, 10.1.130.54-MEN319311, 10.1.130.59-MEN321033, 10.1.130.64-MEN317862, 10.1.130.83-MEN317858, 10.1.135.120-MEN317827, 10.1.135.29-MEN321112, 10.1.135.62-MEN319206, 10.1.140.108-MEN321141, 10.1.140.139-MEN321136, 10.1.140.142-MEN319400, 10.1.140.30-MEN317306, 10.1.140.48-MEN321104, 10.1.140.59-MEN319342, 10.1.140.61-MEN317987, 10.1.140.70-MEN317273, 10.1.140.83-MEN319368, 10.1.140.84-MEN317848, 10.1.140.91-MEN317854, 10.1.145.114-MEN320832, 10.1.145.120-MEN317847, 10.1.145.129-MEN320778, 10.1.145.22-MEN314593, 10.1.145.29-MEN319360, 10.1.145.38-men314548, 10.1.145.48-MEN320795, 10.1.145.92-MEN320839, 10.1.150.104-MEN319324, 10.1.150.105-MEN321901, 10.1.150.108-MEN319406, 10.1.150.110-MEN321149, 10.1.150.111-MEN317756, 10.1.150.112-MEN319433, 10.1.150.113-MEN321146, 10.1.150.114-MEN317302, 10.1.150.119-MEN319374, 10.1.150.123-MEN321106, 10.1.150.127-MEN321156, 10.1.150.130-MEN317457, 10.1.150.147, 10.1.150.28-men314588, 10.1.150.32-MEN319329, 10.1.150.39-MEN317275, 10.1.150.50-MEN317897, 10.1.150.55-MEN320781, 10.1.150.57-MEN319427, 10.1.150.59-MEN319306, 10.1.150.60-MEN321032, 10.1.150.62-MEN319422, 10.1.150.67-men314588, 10.1.150.68-MEN319316, 10.1.150.73-MEN314563, 10.1.150.81-MEN317456, 10.1.150.85-MEN319432, 10.1.150.97-MEN321132, 10.1.155.102-MEN319383, 10.1.155.23, 10.1.155.24-MEN314541, 10.1.155.30-MEN315287, 10.1.155.32-MEN320734, 10.1.155.36-MEN321902, 10.1.155.38-MEN319235, 10.1.155.40-MEN317840, 10.1.155.42-MEN319279, 10.1.155.45-MEN321133, 10.1.155.48-MEN321121, 10.1.155.58-MEN319393, 10.1.155.70-MEN319210, 10.1.155.72-MEN317307, 10.1.155.73-MEN317954, 10.1.155.74-MEN317286, 10.1.155.94-MEN314555, 10.1.160.22-MEN316982, 10.1.4.113-11301CJ, 10.1.4.141-MEN319438, 10.1.4.162-MEN320752, 10.1.4.210-MEN320760, 10.1.4.222-MEN317850, 10.1.4.237-MEN321122, 10.1.4.240-MEN317568, 10.1.4.37-MEN319513, 10.1.4.50-MEN319513, 10.1.4.59, 10.1.4.69-ESTIVENSUAREZ, 10.1.4.70-MEN319661, 10.1.4.76-ESTIVENSUAREZ, 10.1.5.103-MEN317763, 10.1.5.132-MEN321132, 10.1.5.145-MEN319567, 10.1.5.28-MEN321912, 10.1.5.31-MEN321122, 10.1.5.48-MEN319515, 10.1.5.48-MEN321115, 10.1.5.79-MEN321115, 10.1.5.9

Vulnerabilidad	Unencrypted Telnet Server
Riesgo	Medio
Descripción	El host ejecuta un servidor Telnet a través de un canal no cifrado. No se recomienda usar Telnet en un canal sin cifrar, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto no cifrado. Esto permite que un atacante man-in-the-middle espíe una sesión de Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor. Se prefiere SSH a Telnet, ya que protege las credenciales de escuchas ilegales y puede canalizar flujos de datos adicionales, como una sesión X11.
Solución	Deshabilite el servicio Telnet y use SSH en su lugar.
Dispositivos Afectados	10.1.110.45

Vulnerabilidad	Web Server Error Page Information Disclosure
Riesgo	Medio
Descripción	La página de error predeterminada enviada por el host revela información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique el servicio web para que no revele información detallada sobre el servidor web subyacente, o use una página de error personalizada en su lugar.
Dispositivos Afectados	10.1.120.63-MEN317490, 10.1.150.60-MEN321032, 10.1.155.23

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el host 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 servicio web para que no revelen información detallada sobre el servidor web subyacente.
Dispositivos Afectados	10.1.100.29-MEN317263, 10.1.100.30-MEN314492, 10.1.110.27-MEN317813, 10.1.110.61-Men317455, 10.1.110.66-MEN311989, 10.1.110.72-MEN317921, 10.1.110.92-MEN317763, 10.1.115.28-MEN319378, 10.1.115.36-ADMINISTRATIVA, 10.1.115.58-ADMINISTRATIVA, 10.1.120.199-MEN321040, 10.1.120.251-O1APPBK01, 10.1.120.63-MEN317490, 10.1.120.85-MEN317485, 10.1.130.52-RECURSOSHUMANOS, 10.1.145.120-MEN317847, 10.1.150.60-MEN321032, 10.1.155.23, 10.1.4.113-11301CJ, 10.1.4.148-CJ12189, 10.1.4.156-CJ12189, 10.1.5.103-MEN317763, 10.1.5.8-12227CJ, 10.1.5.84-MEN321128, 10.1.5.95-12227CJ

Tabla 10. Vulnerabilidades de severidad Media sobre los segmentos de la LAN

4.2.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Riesgo	Bajo
Descripción	El host utiliza un controlador de dispositivo de red que rellena las tramas de ethernet con datos que varían de un paquete a otro, probablemente tomados de la memoria del kernel, la memoria del sistema asignada al controlador del dispositivo o un búfer de hardware en su tarjeta de interfaz de red. Conocida como 'Etherleak', esta vulnerabilidad de divulgación de información puede permitir que un atacante recopile información confidencial del host afectado, siempre que esté en la misma subred física que ese host.
Solución	Comuníquese con el proveedor del controlador del dispositivo de red para obtener una solución.
Dispositivos Afectados	10.1.120.251

Vulnerabilidad	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
Riesgo	Bajo
Descripción	Según la versión de PHP detectada que se ejecuta en el host es la 5.6.x anterior a la 5.6.35. Por lo tanto, se ve afectado por una vulnerabilidad de derivación de seguridad. Los procesos secundarios de FPM que se pueden volcar permiten eludir los controles de acceso de opcache porque fpm_unix.c realiza una llamada PR_SET_DUMPABLE prctl, lo que permite que un usuario (en un entorno multiusuario) obtenga información confidencial de la memoria de proceso de las aplicaciones PHP de un segundo usuario ejecutando gcore en el PID del Proceso de trabajo de PHP-FPM.
Solución	Actualice a la versión de PHP 5.6.35 o posterior.
Dispositivos Afectados	10.1.110.92-MEN317763, 10.1.5.103-MEN317763

Vulnerabilidad	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
Riesgo	Bajo
Descripción	Según la versión de PHP detectada que se ejecuta en el host es la 5.6.x anterior a la 5.6.35. Por lo tanto, se ve afectado por una vulnerabilidad de derivación de seguridad. Los procesos secundarios de FPM que se pueden volcar permiten eludir los controles de acceso de opcache porque fpm_unix.c realiza una llamada PR_SET_DUMPABLE prctl, lo que permite que un usuario (en un entorno multiusuario) obtenga información confidencial de la memoria de proceso de las aplicaciones PHP de un segundo usuario ejecutando gcore en el PID del Proceso de trabajo de PHP-FPM.

Solución	Actualice a la versión de PHP 5.6.35 o posterior.
Dispositivos Afectados	10.1.110.92-MEN317763, 10.1.5.103-MEN317763

Vulnerabilidad (x3)	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability PHP 7.3.x < 7.3.21 Use-After-Free Vulnerability
Riesgo	Bajo
Descripción	Según la versión de PHP detectada que se ejecuta en el host es la 5.6.x anterior a la 5.6.35. Por lo tanto, se ve afectado por una vulnerabilidad de derivación de seguridad. Los procesos secundarios de FPM que se pueden volcar permiten eludir los controles de acceso de opcache porque fpm_unix.c realiza una llamada PR_SET_DUMPABLE prctl, lo que permite que un usuario (en un entorno multiusuario) obtenga información confidencial de la memoria de proceso de las aplicaciones PHP de un segundo usuario ejecutando gcore en el PID del Proceso de trabajo de PHP-FPM.
Solución	Actualice a la versión de PHP 5.6.35 o posterior.
Dispositivos Afectados	10.1.110.92-MEN317763, 10.1.5.103-MEN317763, 10.1.100.30-MEN314492

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	Comuníquese con el proveedor o consulte la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
Dispositivos Afectados	10.1.130.58-MEN317899, 10.1.150.130-MEN317457, 10.1.150.60-MEN321032, 10.1.150.81-MEN317456

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.
Dispositivos Afectados	10.1.130.58-MEN317899, 10.1.150.130-MEN317457, 10.1.150.60-MEN321032, 10.1.150.81-MEN317456

Vulnerabilidad	SSL Anonymous Cipher Suites Supported
Riesgo	Bajo
Descripción	El host admite el uso de cifrados SSL anónimos. Si bien esto permite que un administrador configure un servicio que encripta 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 intermediario.
Solución	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados débiles.
Dispositivos Afectados	10.1.155.23

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 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.
Dispositivos Afectados	10.1.120.85-MEN317485, 10.1.150.130-MEN317457

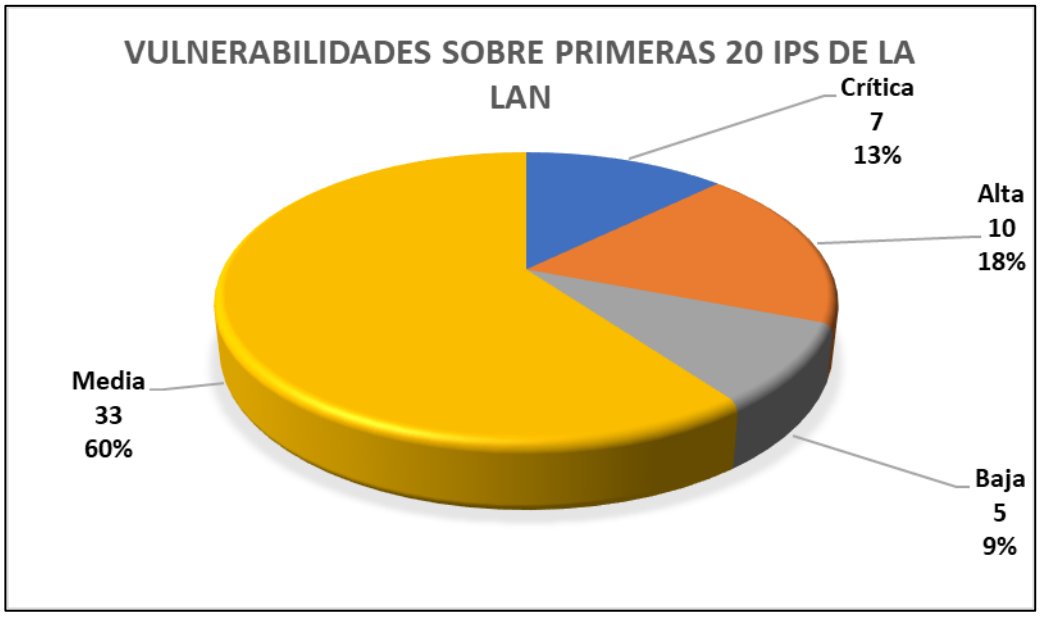
Vulnerabilidad	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Riesgo	Bajo
Descripción	El host permite conexiones SSL/TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede encontrar el texto secreto compartido en poco tiempo (según el tamaño del módulo y los recursos del atacante). Esto puede permitir que un atacante recupere el texto sin formato o potencialmente viole la integridad de las conexiones.
Solución	Vuelva a configurar el servicio para usar módulos Diffie-Hellman únicos de 2048 bits o más.
Dispositivos Afectados	10.1.100.30-MEN314492

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. Cumple con FIPS
Dispositivos Afectados	10.1.100.21-talanquera, 10.1.110.64-MEN3178000, 10.1.115.29-MEN319243, 10.1.120.103-MEN317458, 10.1.120.29-MEN317482, 10.1.120.44-MEN314589, 10.1.120.63-MEN317490, 10.1.120.65-MEN317484, 10.1.120.85-MEN317485

Tabla 11. Vulnerabilidades de severidad Baja sobre los segmentos de la LAN

5. RESUMEN EJECUTIVO CRITICIDAD DE LAS VULNERABILIDADES IDENTIFICADAS

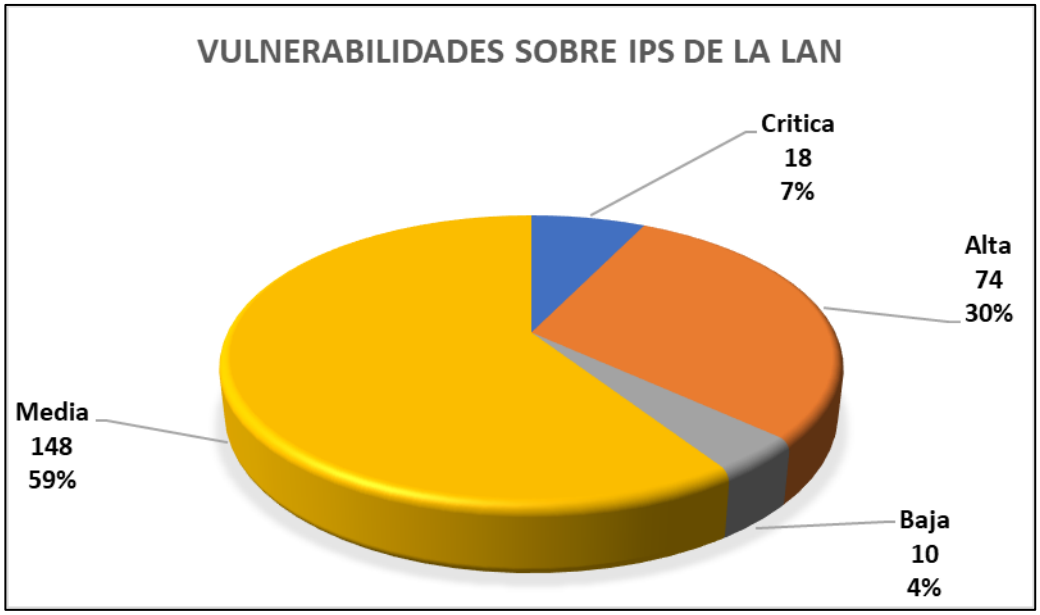
La criticidad de las vulnerabilidades detectadas sobre cada grupo discriminado en la tabla 1, se resume en las gráficas de esta sección. Para el caso del primer grupo que corresponde a las primeras 20 IPs de cada segmento de la LAN, tenemos el siguiente comportamiento en relación a la severidad de las vulnerabilidades encontradas:



Gráfica 1. *Criticidad de las vulnerabilidades detectadas sobre las 20 primeras IPs de la LAN.*

De allí se observa que casi la totalidad de las vulnerabilidades identificadas (60%) tienen una criticidad de nivel medio, seguido de vulnerabilidades de criticidad alta (18%) y crítica (13%).

Para los dispositivos detectados sobre la LAN se obtienen unos resultados similares, en el sentido que predominan las vulnerabilidades de severidad media (59%) seguidas de vulnerabilidades de severidad alta (30%) y crítica (7%) como se puede ver en la siguiente gráfica:



Gráfica 2. *Criticidad de las vulnerabilidades detectadas sobre la LAN.*

6. CONCLUSIONES Y RECOMENDACIONES

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

- Más de la mitad de las vulnerabilidades detectadas sobre la LAN (60% y 59% para cada grupo escaneado respectivamente) corresponden a vulnerabilidades de severidad Media y son principalmente asociadas por cantidad a protocolo SMB y SSL y por variedad a Apache y PHP.

- Se identifican vulnerabilidades asociadas a servicios web y de bases de datos que son servicios que normalmente no esperan verse sobre estaciones de trabajo, ya que este tipo de servicios deberían estar principalmente alojados sobre servidores en alguna DMZ. Por lo cual, se recomienda que desde Mesa de Ayuda se mantenga un control del software instalado y no se instale software que esté fuera de la línea base que tiene definido el Ministerio para las estaciones de trabajo.

- Se recomienda que el proceso de mitigación inicie por las vulnerabilidades de severidad crítica y alta que son las que mayor riesgo generan sobre la red del ministerio y para las cuales normalmente existen *exploits* disponibles, por lo que la probabilidad de ser explotadas es mayor y la materialización del riesgo representaría un impacto sobre la red del Ministerio.

- Se recomienda que el proceso de mitigación inicie también por los equipos que aportan la mayor cantidad de vulnerabilidades que particularmente corresponden a las placas MEN317763 y MEN314492.

- Se recomienda que la operación mantenga actualizado un inventario de los dispositivos conectados sobre el intervalo de red que no hace parte del direccionamiento provisto por el DHCP y que debería estar destinado a dispositivos que no sean estaciones de trabajo.

- El escaneo a las estaciones de trabajo de usuarios tiene diferentes variables, como que la cantidad detectada de equipos por cada escaneo es variable e incluso el resultado específico sobre un equipo en particular puede variar entre uno y otro escaneo en cuanto a que pueden presentarse situaciones en las que un usuario pudo haber apagado/suspendido el equipo justo en medio del escaneo o que puedo cambiar de medio de conexión (red cableada a red inalámbrica o viceversa), por lo cual, fue necesario compilar diferentes resultados.

7. ANEXOS

- Equipos20IPs.xlsx
- EquiposLAN_Usuarios.xlsx
- Trimestre5_20IPs_LAN.html
- Trimestre5_LAN_primero.html
- Trimestre5_LAN_segundo.html
- Trimestre5_LAN_tercero.html

Información del documento

Fecha	Versión	Responsable	Revisado por	Aprobado por
25/02/2022	2.0	Especialista seguridad informática	Líder de Gestión técnica y seguridad	

Control de cambios

Fecha	Versión	Causa Cambio	Responsable
11/02/2022	1.0	Creación del Documento	Especialista seguridad informática
25/02/2022	2.0	Ajuste a documento de acuerdo a comunicado INT-UT-COM-0222-1003	Especialista seguridad informática