Boletín de febrero de 2020

Avisos Técnicos

Vulnerabilidad de desbordamiento de búfer en sudo

Fecha de publicación: 03/02/2020

Importancia: Alta

Recursos afectados:

Versiones de *sudo*, desde 1.7.1 hasta 1.8.25p1, si la opción *pwfeedback* está habilitada en el archivo *sudoers*.

Descripción:

Joe Vennix ha descubierto una vulnerabilidad de criticidad alta en *sudo*, que podría permitir a un atacante desencadenar un desbordamiento de búfer basado en pila (*stack*).

Solución:

Actualizar a la versión 1.8.31.

Detalle:

Una vulnerabilidad en *sudo*, de tipo desbordamiento de búfer basado en pila (*stack*), permitiría a un usuario no privilegiado realizar una escalada de privilegios y obtener permisos de *root*, lo que le otorgaría el control completo de la información en las versiones afectadas con la opción *pwfeedback* activada en el archivo *sudoers*. Se ha asignado el identificador CVE-2019-18634 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Múltiples vulnerabilidades en Squid

Fecha de publicación: 04/02/2020

Importancia: Alta

Recursos afectados:

Las siguientes versiones de Squid:

- desde la 2.x hasta la 2.7.STABLE9;
- desde la 3.x hasta la 3.5.28;
- desde la 4.x hasta la 4.9.

Descripción:

Se han detectado tres vulnerabilidades en múltiples versiones del servidor proxy Squid que podrían permitir a un atacante omitir los controles de seguridad de acceso, la denegación del servicio o la divulgación de información.

Solución:

Actualizar a la versión 4.10.

Detalle:

- Debido a una incorrecta validación de la entrada, Squid puede interpretar las solicitudes HTTP, específicamente diseñadas, de manera errónea para acceder a los recursos del servidor prohibidos por los anteriores filtros de seguridad. Además, debido a la incorrecta administración del búfer, un cliente remoto puede causar una condición de desbordamiento de búfer en un Squid que actúa como proxy inverso. Se han reservado los identificadores CVE-2020-8449 y CVE-2020-8450 para esta vulnerabilidad.

- Debido a la gestión incorrecta de los datos, Squid es vulnerable a la divulgación de información cuando traduce los listados del servidor FTP a respuestas HTTP. Se ha reservado el identificador CVE-2019-12528 para esta vulnerabilidad.
- Debido a la incorrecta gestión del búfer, el archivo binario *ext_lm_group_acl* es vulnerable a un ataque de denegación de servicio cuando se procesan las credenciales de autenticación NTLM (*NT LAN Manager*). Se ha reservado el identificador CVE-2020-8517 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 06/02/2020

Importancia: Alta

Recursos afectados:

- ASR 9000 Series Aggregation Services Routers;
- Carrier Routing System (CRS);
- Firepower 4100 Series;
- Firepower 9300 Security Appliances;
- IOS XRv 9000 Router;
- MDS 9000 Series Multilayer Switches;
- Network Convergence System (NCS) Series Routers:
  - 540 Series Routers;
  - 560 Series Routers;
  - 1000 Series;
  - 5000 Series;
  - 5500 Series;
  - 6000 Series;
- Nexus 1000 Virtual Edge para VMware vSphere;
- Nexus 1000V Switch para Microsoft Hyper-V;
- Nexus 1000V Switch para VMware vSphere;
- Nexus 3000 Series Switches;
- Nexus 5500 Plataform Switches;
- Nexus 5600 Plataform Switches;
- Nexus 6000 Series Switches;
- Nexus 7000 Series Switches;
- Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI);
- Nexus 9000 Series Switches en modo independiente NX-OS:
- UCS 6200 Series Fabric Interconnects;
- UCS 6300 Series Fabric Interconnects;
- UCS 6400 Series Fabric Interconnects;
- Network Convergence System (NCS) Series Routers:
  - 1000;
  - 5000;
  - 5500;
  - 6000;
- Video Surveillance 3000 Series IP Cameras;
- Video Surveillance 4000 Series High-Definition IP Cameras;
- Video Surveillance 4300E and 4500E High-Definition IP Cameras;
- Video Surveillance 6000 Series IP Cameras;
- Video Surveillance 7000 Series IP Cameras;
- Video Surveillance PTZ IP Cameras;
- IP Conference Phone 7832;
- IP Conference Phone 7832 con firmware multiplataforma;
- IP Conference Phone 8832;
- IP Conference Phone 8832 con firmware multiplataforma;
- IP Phone 6821, 6841, 6851, 6861, 6871 con firmware multiplataforma;
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones;
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones con firmware multiplataforma;
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones;
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones con firmware multiplataforma;
- Unified IP Conference Phone 8831;
- Unified IP Conference Phone 8831 para control de llamada de terceros;
- Wireless IP Phone 8821, 8821-EX.

Descripción:

Dos investigadores de Armis, Barak Hadad y Ben Seri, han notificado a Cisco cinco vulnerabilidades de criticidad alta. Un atacante próximo, no autenticado, podría generar una condición de denegación de servicio, ejecución de código arbitrario, incluso con privilegios de *root*, y ocasionar reinicios en los dispositivos.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software de Cisco.

Detalle:

- Una falta de comprobación en el procesamiento de los mensajes de Cisco Discovery Protocol, podrían permitir a un atacante próximo, no autenticado, enviar paquetes maliciosos y ocasionar reinicios o generar una condición de denegación de servicio (DoS) en el dispositivo. Se ha asignado el identificador CVE-2020-3120 para esta vulnerabilidad.
- Un validación incorrecta de las cadenas de entrada en ciertos campos de los mensajes de Cisco Discovery Protocol, podrían permitir a un atacante próximo, no autenticado, enviar paquetes maliciosos y ocasionar la ejecución arbitraria de código con privilegios administrativos en el dispositivo. Se ha asignado el CVE-2020-3118 para esta vulnerabilidad.
- Una falta de comprobación en el procesamiento de los mensajes de Cisco Discovery Protocol, podrían permitir a un atacante próximo, no autenticado, enviar paquetes maliciosos y ocasionar reinicios o generar una condición de denegación de servicio (DoS) en el dispositivo. Se ha asignado el identificador CVE-2020-3110 para esta vulnerabilidad.
- Una incorrecta validación de los campos de ciertas entradas de los mensajes de Cisco Discovery Protocol, podrían permitir a un atacante próximo, no autenticado, enviar paquetes maliciosos y ocasionar la ejecución arbitraria de código con privilegios administrativos en el dispositivo. Se ha asignado el identificador CVE-2020-3119 para esta vulnerabilidad.

- Una falta de comprobación en el procesamiento de los mensajes de Cisco Discovery Protocol, podrían permitir a un atacante próximo, no autenticado, enviar paquetes maliciosos y ocasionar reinicios, generar una condición de denegación de servicio (DoS), o la ejecución arbitraria de código con privilegios de *root* en el dispositivo. Se ha asignado el identificador CVE-2020-3111 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad en switches de Aruba

Fecha de publicación: 12/02/2020

Importancia: Alta

Recursos afectados:

Aruba Intelligent Edge Switches:

- 5400R,
- 3810,
- 2920,
- 2930,
- 2530 con GigT Port,
- 2530 10/100 port,
- 2540.

Para las siguientes versiones de firmware:

- 16.08.*, anteriores a la 16.08.0009;
- 16.09.*, anteriores a la 16.09.0007;
- 16.10.*, anteriores a la 16.10.0003.

Descripción:

Se ha publicado una vulnerabilidad en productos Aruba que podrían permitir a un atacante remoto la divulgación de información.

Solución:

Actualizar a las siguientes versiones de *firmware*:

- 16.08.0009,
- 16.09.0007,
- 16.10.0003.

Detalle:

Una vulnerabilidad de divulgación de información en la interfaz de gestión de la web de los switches afectados podría permitir a un atacante remoto recuperar información del sistema, enviando un paquete especialmente elaborado a dicho interfaz. Bajo condiciones muy específicas, la vulnerabilidad podría ser explotada sin necesidad de autenticación. Se ha reservado el identificador CVE-2019-5322 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de febrero de 2020

Fecha de publicación: 12/02/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge (basado en Chromium);
- ChakraCore;
- Internet Explorer;
- Microsoft Exchange Server;
- Microsoft SQL Server;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Windows Malicious Software Removal Tool;
- Windows Surface Hub.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de febrero, consta de 101 vulnerabilidades, 13 clasificadas como críticas y 88 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de Microsoft se informa de los distintos métodos para llevar a cabo dichas actualizaciones.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- ejecución remota de código,

- escalada de privilegios,
- denegación de servicio,
- divulgación de información,
- omisión de característica de seguridad,
- suplantación de identidad (*spoofing*),
- manipulación de información (*tampering*).

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Vulnerabilidad en subsistemas CSME de Intel

Fecha de publicación: 12/02/2020

Importancia: Alta

Recursos afectados:

- Intel CSME versiones anteriores a:
  - 12.0.49;
  - 12.0.56, solo para IOT;
  - 13.0.21;
  - 14.0.11.

Descripción:

El investigador, Chedva Gottesman, trabajando conjuntamente con Intel, ha descubierto una vulnerabilidad de criticidad alta en subsistemas CSME que podría permitir a un atacante local realizar una escalada de privilegios, una condición de denegación de servicio o divulgar información.

Solución:

Actualizar CSME a las versiones:

- 2.0.49,
- 13.0.21,
- 14.0.11.

o posterioes.

- Para CSME IOT, actualizar a la versión 12.0.56 o posterior.

Detalle:

Una autenticación incorrecta podría permitir a un atacante local realizar una escalada de privilegios, una condición de denegación de servicio o divulgar información. Se ha reservado el identificador CVE-2019-14598 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de febrero de 2020

Fecha de publicación: 12/02/2020

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5;
- SAP Host Agent, version 7.21;
- SAP Landscape Management, versión 3.0;
- ABAP Server (utilizado en NetWeaver y Suite/ERP), versiones;
  - utilizando Kernel 7.21 o 7.22, que usa ABAP Server desde 7.00 hasta 7.31;
  - utilizando Kernel 7.45, 7.49 o 7.53, que usa ABAP Server desde 7.40 hasta 7.52;
  - ABAP Platform.
- SAP ERP, versiones SAP_APPL 600, 602, 603, 604, 605, 606, 616, SAP_FIN 617, 618, 700, 720 y 730;
- SAP S/4 HANA, versiones:
  - S4CORE 100, 101, 102, 103, 104;
  - SAP_BASIS 7.50, 7.51, 7.52, 7.53, 7.54.
- SAP NetWeaver, versiones:
  - 7.30, 7.31, 7.40 y 7.50 (Knowledge Management ICE Service);
  - SAP_BASIS 7.40;
  - SAP_BASIS 702, 730, 731 y 740;
  - 7.30, 7.31, 7.40 y 7.50 (Heap Dump Application);
  - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50 (Guided Procedures).
- SAP Business Objects Business Intelligence Platform (CMC), versión 4.2;
- SAP Mobile Platform, versión 3.0.

Descripción:

SAP ha publicado varias actualizaciones de seguridad de diferentes productos en su comunicado mensual.

Solución:

Visitar el portal de soporte de SAP e instalar las actualizaciones o los parches necesarios, según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 13 notas de seguridad y 2 actualizaciones, siendo una de las actualizaciones de severidad crítica, 3 notas de severidad alta, y la otra actualización, junto con el resto de notas, de severidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de DoS (*Denial of Service*);
- 2 vulnerabilidades de falta de comprobación de datos de entrada;
- 2 vulnerabilidades de XSS (*Cross-Site Scripting*);
- 1 vulnerabilidad de falta de comprobación de autenticación;
- 1 vulnerabilidad de división de respuesta HTTP;
- 6 vulnerabilidades de otro tipo.

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-6186, CVE-2020-6191, CVE-2020-6192, CVE-2020-6188, CVE-2020-6193, CVE-2020-6184, CVE-2020-6185, CVE-2020-6181, CVE-2020-6190, CVE-2020-6183, CVE-2020-6189, CVE-2020-6187 y CVE-2020-6177. El identificador CVE-2019-0271 se ha asignado.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad de omisión de autenticación en IBM Tivoli Monitoring Service

Fecha de publicación: 13/02/2020

Importancia: Alta

Recursos afectados:

IBM Tivoli Monitoring Service, versiones:

- 6.3.0 Fix Pack 7, Service Packs 1 y 2;
- desde la 6.3.0.7-TIV-ITM_TEMA-IF0003 hasta la 6.3.0.7-TIV-ITM_TEMA-IF0009.

Descripción:

Ehsan Razaghi ha reportado una vulnerabilidad, de severidad alta, que afecta al producto Tivoli Monitoring Service de IBM.

Solución:

Actualizar IBM Tivoli Monitoring Service a la versión 6.3.0 Fix Pack 7 Service Pack 3 (6.3.0.7-TIV-ITM-SP0003).

Detalle:

Una omisión de autenticación en IBM Tivoli Monitoring Service podría permitir a un atacante acceder y modificar los aspectos operativos del servidor de monitorización del ITM, lo que conduciría a una condición de denegación de servicio o a la desactivación del servidor de monitorización. Se ha reservado el identificador CVE-2019-4592 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Insuficiente protección ante CSRF en Expedition Migration Tool de Palo Alto

Fecha de publicación: 13/02/2020

Importancia: Alta

Recursos afectados:

Expedition Migration Tool, versión 1.1.51 y anteriores.

Descripción:

El investigador, Jimi Sebree de Tenable, ha descubierto una vulnerabilidad de criticidad alta. Un atacante remoto, no autenticado, podría secuestrar la autenticación de los administradores y realizar acciones en la herramienta.

Solución:

Actualizar Expedition Migration Tool a la versión 1.1.52 o posterior.

Detalle:

Una insuficiente protección ante Cross-Site Request Forgery (CSRF), podría permitir a atacante remoto, no autenticado, secuestrar la autenticación de los administradores y realizar acciones en la herramienta.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Db2 de IBM

Fecha de publicación: 19/02/2020

Importancia: Alta

Recursos afectados:

Todos los fix pack de IBM Db2, en todas las plataformas, versiones V9.7, V10.1, V10.5, V11.1 y V11.5.

Descripción:

Se han publicado varias vulnerabilidades en productos Db2 de IBM que podrían permitir a un atacante denegar el servicio o ejecutar código arbitrario con privilegios de *root*.

Solución:

Aplicar la actualización correspondiente para cada versión. Para más detalles, consultar la sección de *Referencias*.

Detalle:

- El envío de paquetes, especialmente diseñados, podría permitir a un atacante, no autenticado, denegar el servicio a través de un uso excesivo de memoria. Se ha asignado el identificador CVE-2020-4135 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer, causada por una comprobación de los límites inadecuada, podría permitir a un atacante local ejecutar código arbitrario en el sistema, con privilegios de *root*. Se ha asignado el identificador CVE-2020-4204 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de inyección SQL en múltiples productos de IBM

Fecha de publicación: 20/02/2020

Importancia: Alta

Recursos afectados:

- IBM Emptoris Spend Analysis, versiones:
  - 10.1.0.x;
  - 10.1.1.x;
  - 10.1.3.x.
- IBM Emptoris Strategic Supply Management Platform, versiones:
  - 10.1.0.x;
  - 10.1.1.x;
  - 10.1.3.x.

Descripción:

Los productos IBM Emptoris Spend Analysis e IBM Emptoris Strategic Supply Management Platform contienen una vulnerabilidad, de severidad alta, de tipo inyección SQL.

Solución:

- IBM Emptoris Spend Analysis, actualizar a las versiones:
  - 10.1.0.34;
  - 10.1.1.33;
  - 10.1.3.29.
- IBM Emptoris Strategic Supply Management Platform, actualizar a las versiones:
  - 10.1.0.34;
  - 10.1.1.33;
  - 10.1.3.29.

Detalle:

Un atacante remoto podría enviar peticiones SQL, especialmente elaboradas, que podrían permitirle ver, añadir, modificar o eliminar información en la base de datos del *backend*. Se ha reservado el identificador CVE-2019-4752 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 20/02/2020

Importancia: Crítica

Recursos afectados:

- Cisco Smart Software Manager On-Prem, versiones anteriores a 7-202001 con la opción High Availability (HA) activada;
- Cisco Unified Contact Center Express Software, versiones anteriores a 12.5(1);
- Firepower Management Center (FMC) 1000;
- Firepower Management Center (FMC) 2500;
- Firepower Management Center (FMC) 4500;
- Secure Network Server 3500 Series Appliances;
- Secure Network Server 3600 Series Appliances;
- Threat Grid 5504 Appliance;
- Cisco ESA y Cisco SMA, dispositivos virtuales y de hardware, cuando están ejecutando una versión vulnerable del software Cisco AsyncOS configurada para utilizar Cisco AMP o seguimiento de mensajes;
- Cisco AsyncOS Software, versiones 12.1.0-085 y 11.1.0-131 para Cisco Email Security Appliance (ESA);
- Cisco DCNM software, versiones anteriores a la Release 11.3(1).

Descripción:

Se han identificado múltiples vulnerabilidades en productos Cisco, 1 de severidad crítica y 6 de severidad alta.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

- Una cuenta del sistema con contraseña estática y por defecto podría permitir a un atacante remoto, no autenticado, acceder a información sensible del sistema con una cuenta con privilegios elevados. Se ha asignado el identificador CVE-2020-3158 para esta vulnerabilidad.
- Las restricciones insuficientes durante la subida de contenidos podrían permitir a un atacante remoto, no autenticado, cargar archivos arbitrarios y ejecutar comandos en el sistema operativo subyacente. Se ha asignado el identificador CVE-2019-1888 para esta vulnerabilidad.
- La validación insuficiente de las imágenes del servidor para la actualización del firmware podrían permitir a un atacante físico, no autenticado, evadir las comprobaciones de arranque seguro Unified Extensible Firmware Interface (UEFI) y cargar una imagen de software comprometida en un dispositivo afectado. Se ha asignado el identificador CVE-2019-1736 para esta vulnerabilidad.
- La validación insuficiente de los adjuntos de correos electrónicos podría permitir a un atacante remoto, no autenticado, enviar adjuntos especialmente diseñados para causar múltiples cierres inesperados en procesos internos del producto, provocando una denegación del servicio. Se ha asignado el identificador CVE-2019-1983 para esta vulnerabilidad.
- La validación inadecuada de los mensajes de correo electrónico con adjuntos de gran tamaño podría permitir a un atacante remoto, no autenticado, aumentar la utilización de CPU hasta el 100%, provocando una denegación del servicio. Se ha asignado el identificador CVE-2019-1947 para esta vulnerabilidad.
- Una insuficiente validación en el control de acceso podría permitir a un atacante remoto, no autenticado, escalar privilegios en la aplicación mediante el envío de peticiones especialmente diseñadas a la REST API. Se ha asignado el identificador CVE-2020-3112 para esta vulnerabilidad.
- La protección CSRF insuficiente de la interfaz web, podría permitir a un atacante remoto, no autenticado, realizar ataques cross-site request forgery en el sistema y conseguir llevar a cabo acciones arbitrarias con los mismos permios que el usuario afectado. Se ha asignado el identificador CVE-2020-3114 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en vRealize Operations para Horizon Adapter de VMware

Fecha de publicación: 20/02/2020

Importancia: Crítica

Recursos afectados:

vRealize Operations para Horizon Adapter, versiones:

- 6.6.x;
- 6.7.x.

Descripción:

Se han identificado 3 vulnerabilidades, de severidad crítica, alta y media, de ejecución remota de código, omisión de autenticación y divulgación de información, respectivamente.

Solución:

Actualizar el producto afectado a las versiones:

- 6.6.1;
- 6.7.1.

Detalle:

- Un atacante remoto, no autenticado, que tenga acceso a la red de vRealize Operations, con Horizon Adapter en funcionamiento, podría ejecutar código arbitrario en vRealize Operations. Se ha asignado el identificador CVE-2020-3943 para esta vulnerabilidad.
- Un atacante remoto, no autenticado, que tenga acceso a la red de vRealize Operations, con Horizon Adapter en funcionamiento, podría omitir la autenticación de Horizon Adapter, aprovechando una configuración inadecuada del repositorio de confianza (*trust store*) de entidades certificadoras. Se ha asignado el identificador CVE-2020-3944 para esta vulnerabilidad.

Se ha asignado el identificador CVE-2020-3945 para la vulnerabilidad de severidad media.

Etiquetas: Actualización, VMware, Vulnerabilidad

Vulnerabilidad de Cross-Site Scripting en TIBCO EBX

Fecha de publicación: 20/02/2020

Importancia: Alta

Recursos afectados:

- TIBCO EBX, versiones:
  - 5.8.1.fixS y anteriores;
  - 5.9.3, 5.9.4, 5.9.5, 5.9.6 y 5.9.7.
- El componente Web server.

Descripción:

Se ha publicado una vulnerabilidad, de severidad alta, que podría permitir a un atacante, no autenticado, realizar ataques cross-site scripting almacenado.

Solución:

Actualizar a las siguientes versiones:

- TIBCO EBX, versiones 5.8.1.fixT o siguientes;
- TIBCO EBX, versiones 5.9.8 o siguientes.

Detalle:

Una vulnerabilidad presente en los productos afectados, podría permitir a un atacante, no autenticado, realizar ataques cross-site scripting almacenado. Se ha asignado el identificador CVE-2019-17333 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades de inyección de comandos en IBM Spectrum Protect Plus

Fecha de publicación: 24/02/2020

Importancia: Crítica

Recursos afectados:

IBM Spectrum Protect Plus, versiones desde 10.1.0 hasta 10.1.5.

Descripción:

Múltiples vulnerabilidades, todas de severidad crítica y de tipo inyección de comandos, podrían permitir a un atacante remoto ejecutar código arbitrario en el sistema afectado.

Solución:

Actualizar IBM Spectrum Protect Plus a la versión 10.1.5 *patch1*.

Detalle:

Varias vulnerabilidades en IBM Spectrum Protect Plus, de tipo inyección de comandos, podrían permitir a un atacante remoto ejecutar código arbitrario en el sistema, mediante el uso de un comando HTTP especialmente diseñado. Se han reservado los identificadores CVE-2020-4210, CVE-2020-4213, CVE-2020-4222, CVE-2020-4212 y CVE-2020-4211 para estas vulnerabilidades.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad en SyncIQ de Isilon OneFS de Dell

Fecha de publicación: 24/02/2020

Importancia: Crítica

Recursos afectados:

Dell EMC Isilon OneFS, todas las versiones hasta la 8.2.2.

Descripción:

Dell ha detectado una vulnerabilidad de severidad crítica en SyncIQ que podría permitir a un atacante remoto el acceso no autorizado al sistema.

Solución:

Dell ha publicado diversas actualizaciones y recomendaciones en función de la versión y características del producto. Para más información consultar el apartado de *Referencias*.

Detalle:

La vulnerabilidad afecta a las versiones de OneFS que dispongan de SyncIQ. Un atacante remoto podría obtener acceso no autorizado y realizar acciones en el sistema. Se ha reservado el identificador CVE-2020-5328 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en AJP de Apache Tomcat

Fecha de publicación: 25/02/2020

Importancia: Alta

Recursos afectados:

Apache Tomcat, versiones:

- desde 7.0.0 hasta 7.0.99,
- desde 8.5.0 hasta 8.5.50,
- desde 9.0.0.M1 hasta 9.0.30.

Descripción:

El equipo de seguridad de Apache Tomcat detectó una vulnerabilidad, de severidad alta, en Apache JServ Protocol (AJP), que podría permitir a un atacante realizar una ejecución remota de código.

Solución:

Actualizar a las siguientes versiones:

- 7.0.100,
- 8.5.51,
- 9.0.31.

Detalle:

Apache Tomcat trata las conexiones AJP como si tuvieran un mayor nivel de confianza que, por ejemplo, una conexión similar de HTTP. Si un atacante tuviera acceso a esas conexiones, podría realizar una ejecución remota de código que le otorgaría acceso a archivos arbitrarios de cualquier parte de la aplicación web. Se ha asignado el identificador CVE-2020-1938 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades en OpenSMTPD

Fecha de publicación: 26/02/2020

Importancia: Crítica

Recursos afectados:

OpenBSD 6.6.

Descripción:

Se han publicado múltiples vulnerabilidades, de severidades crítica y baja, en OpenBSD que podrían permitir a un atacante remoto tomar el control de un servidor afectado o la divulgación de información local.

Solución:

Actualizar a la versión 6.6.4p1.

Detalle:

- La vulnerabilidad de severidad baja podría permitir a un atacante local, sin privilegios, leer la primera línea de un archivo arbitrario (por ejemplo, el hash de la contraseña de root en */etc/master.passwd*) o el contenido del archivo de otro usuario (si este archivo y */var/spool/smtpd/* están en el mismo sistema de archivos). Esta vulnerabilidad generalmente no es explotable en Linux, ya que */proc/sys/fs/protected_hardlinks* es "1" por defecto en la mayoría de las distribuciones, sin embargo si es explotable en Fedora. Se ha asignado el identificador CVE-2020-8793 para esta vulnerabilidad.
- La vulnerabilidad de severidad crítica consiste en una lectura fuera de límites en *smtpd* que podría permitir a un atacante remoto inyectar comandos arbitrarios en archivos que luego se ejecutan como *root*. Por otra parte, la falta de revocación de privilegios en el *smtpctl* permite ejecutar comandos con el grupo *_smtpq*. Se ha asignado el identificador CVE-2020-8794 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 27/02/2020

Importancia: Alta

Recursos afectados:

- Firepower
  - 1000 Series;
  - 2100 Series;
  - 4100 Series;
  - 9300 Security Appliances.
- Nexus
  - 1000 Virtual Edge para VMware vSphere;
  - 1000V Switch para Microsoft Hyper-V;
  - 1000V Switch para VMware vSphere;
  - 3000 Series Switches;
  - 5500 Platform Switches;
  - 5600 Platform Switches;
  - 6000 Series Switches;
  - 7000 Series Switches;
  - 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI);
  - 9000 Series Switches en modo NX-OS independiente.
- UCS
  - 6200 Series Fabric Interconnects;
  - 6300 Series Fabric Interconnects;

    - 6400 Series Fabric Interconnects.
- MDS 9000 Series Multilayer Switches.

Descripción:

Se han identificado 6 vulnerabilidades en productos Cisco, todas de severidad alta, de ejecución de código arbitraria, denegación de servicio e inyección de comandos.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

- Un atacante adyacente, no autenticado, podría ejecutar código arbitrario como *root* o generar una condición de denegación de servicio (DoS), debido a una validación insuficiente en las cabeceras de los paquetes de los productos afectados. Se ha asignado el identificador CVE-2020-3172 para esta vulnerabilidad.
- Una vulnerabilidad en la gestión local del CLI (*Command Line Interface*), debido a una insuficiente validación de entrada, permitiría a un atacante local, no autenticado, ejecutar comandos arbitrarios. Se ha asignado el identificador CVE-2020-3171 para esta vulnerabilidad.
- Un atacante local, no autenticado, podría explotar la vulnerabilidad presente en CLI y ejecutar comandos arbitrarios en el producto afectado. Se ha asignado el identificador CVE-2020-3167 para esta vulnerabilidad.
- Un control impropio del uso de los recursos permitiría a un atacante remoto, no autenticado, causar una condición de denegación de servicio (DoS) en el sistema afectado. Se ha asignado el identificador CVE-2020-3175 para esta vulnerabilidad.
- Un atacante remoto, no autenticado, podría generar una condición de denegación de servicio (DoS) debido a la asignación incorrecta de recursos durante los intentos fallidos de inicio de sesión del CLI. Se ha asignado el identificador CVE-2020-3168 para esta vulnerabilidad.
- Una validación insuficiente en los argumentos de los comandos permitiría a un atacante local, autenticado, ejecutar comandos arbitrarios en el dispositivo afectado. Se ha asignado el identificador CVE-2020-3173 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad