Boletín de marzo de 2020

Avisos Técnicos

Deserialización de datos no confiables en productos Dell

Fecha de publicación: 03/03/2020

Importancia: Crítica

Recursos afectados:

- Dell EMC Avamar Server, versiones 7.4.1, 7.5.0, 7.5.1, 18.2, 19.1 y 19.2;
- Dell EMC Integrated Data Protection Appliance (IDPA), versiones 2.0, 2.1, 2.2, 2.3, 2.4 y 2.4.1.

Descripción:

Se ha publicado una vulnerabilidad en Dell EMC Avamar Server y en Dell EMC Integrated Data Protection Appliance que podría permitir a un atacante comprometer el sistema afectado.

Solución:

Aplicar los siguientes hotfix en función de la versión afectada:

- Dell EMC Avamar Server 7.4.1 ? HOTFIX 316625,
- Dell EMC Avamar Server 7.5.0 ? HOTFIX 316626,
- Dell EMC Avamar Server 7.5.1 ? HOTFIX 316627,
- Dell EMC Avamar Server 18.2 ? HOTFIX 316484,
- Dell EMC Avamar Server 19.1 ? HOTFIX 316485,
- Dell EMC Avamar Server 19.2 ? HOTFIX 316691,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.0 ? HOTFIX 316625,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.1 ? HOTFIX 316626,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.2 ? HOTFIX 316627,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.3 ? HOTFIX 316484,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.4 ? HOTFIX 316484,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.4.1 ? HOTFIX 316484.

Detalle:

Una vulnerabilidad de deserialización de datos no confiables podría permitir a un atacante remoto, no autenticado, enviar un *payload* serializado que ejecute código en el sistema. Se ha reservado el identificador CVE-2020-5341 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Divulgación de información en OneView Global Dashboard de HPE

Fecha de publicación: 04/03/2020

Importancia: Alta

Recursos afectados:

HPE OneView Global Dashboard, versión 1.9.

Descripción:

HPE ha detectado una vulnerabilidad de criticidad alta. Un atacante remoto podría revelar información del sistema.

Solución:

Actualizar HPE OneView Global Dashboard a la versión 1.91.

Detalle:

Tras la instalación de la versión 1.9 de OneView Global Dashboard, el dispositivo podría dejar los puertos del firewall abiertos. Un atacante remoto podría revelar información del sistema. Se ha reservado el identificador CVE-2020-7130 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 04/03/2020

Importancia: Crítica

Recursos afectados:

- R7800, ejecutando versiones de *firmware* anteriores a 1.0.2.68;
- R6400v2, ejecutando versiones de *firmware* anteriores a 1.0.4.84;
- R6700, ejecutando versiones de *firmware* anteriores a 1.0.2.8;
- R6700v3, ejecutando versiones de *firmware* anteriores a 1.0.4.84;
- R6900, ejecutando versiones de *firmware* anteriores a 1.0.2.8;
- R7900, ejecutando versiones de *firmware* anteriores a 1.0.3.10;
- D6220, ejecutando versiones de *firmware* anteriores a 1.0.0.52;
- D6400, ejecutando versiones de *firmware* anteriores a 1.0.0.86;
- D7000v2, ejecutando versiones de *firmware* anteriores a 1.0.0.53;
- D8500, ejecutando versiones de *firmware* anteriores a 1.0.3.44;
- R6220, ejecutando versiones de *firmware* anteriores a 1.1.0.80;
- R6250, ejecutando versiones de *firmware* anteriores a 1.0.4.34;
- R6260, ejecutando versiones de *firmware* anteriores a 1.1.0.64;
- R6400, ejecutando versiones de *firmware* anteriores a 1.0.1.46;
- R6700v2, ejecutando versiones de *firmware* anteriores a 1.2.0.36;
- R6800, ejecutando versiones de *firmware* anteriores a 1.2.0.36;
- R6900P, ejecutando versiones de *firmware* anteriores a 1.3.1.64;
- R6900v2, ejecutando versiones de *firmware* anteriores a 1.2.0.36;
- R7000, ejecutando versiones de *firmware* anteriores a 1.0.9.42;
- R7000P, ejecutando versiones de *firmware* anteriores a 1.3.1.64;
- R7100LG, ejecutando versiones de *firmware* anteriores a 1.0.0.50;
- R7300DST, ejecutando versiones de *firmware* anteriores a 1.0.0.70;
- R7900P, ejecutando versiones de *firmware* anteriores a 1.4.1.30;
- R8000, ejecutando versiones de *firmware* anteriores a 1.0.4.28;
- R8000P, ejecutando versiones de *firmware* anteriores a 1.4.1.30;
- R8300, ejecutando versiones de *firmware* anteriores a 1.0.2.128;
- R8500, ejecutando versiones de *firmware* anteriores a 1.0.2.128;
- R8900, ejecutando versiones de *firmware* anteriores a 1.0.4.12;
- R9000, ejecutando versiones de *firmware* anteriores a 1.0.4.12;
- XR500, ejecutando versiones de *firmware* anteriores a 2.3.2.32.

Descripción:

Netgear ha publicado 3 vulnerabilidades, 1 de severidad crítica y 2 de severidad alta, que afectan a sus productos.

Solución:

Acceder a la página de soporte de Netgear y descargar la última versión del *firmware* del dispositivo afectado.

Detalle:

- La vulnerabilidad de severidad crítica permitiría a un atacante remoto realizar una ejecución de código sin autenticación.
- Se ha identificado una vulnerabilidad, con severidad alta, de tipo inyección de comandos previa a la autenticación.
- Se ha identificado otra vulnerabilidad, también de severidad alta, de tipo inyección de comandos posterior a la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 05/03/2020

Importancia: Alta

Recursos afectados:

- Cisco Prime Network Registrar, todas las versiones anteriores a la 10.1;
- Cisco Webex Meetings, todas las versiones de Webex Network Recording Player y Webex Player, anteriores a las versiones WBS 39.5.17 o WBS 39.11.0;
- Cisco Webex Meetings Online, todas las versiones de Webex Network Recording Player y Webex Player, anteriores a la versión 1.3.49;
- Cisco Webex Meetings Server, todas las versiones de Webex Network Recording Player, anteriores a las versiones 3.0MR3SecurityPatch1 y 4.0MR2SecurityPatch2;
- Aplicación Cisco Intelligent Proximity;
- Cisco Jabber;
- Cisco Webex Meetings;
- Cisco Webex Teams;
- Cisco Meeting App.

Descripción:

Cisco, trabajando conjuntamente con varios investigadores, ha detectado cuatro vulnerabilidades de criticidad alta que afectan a múltiples productos. Un atacante remoto, no autenticado, podría ejecutar código arbitrario, interceptar tráfico o modificar las configuraciones del dispositivo.

Solución:

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

Detalle:

- Cisco Webex Network Recording Player y Cisco Webex Player, ambas en sus versiones para Microsoft Windows, contienen dos vulnerabilidades que son debidas a una validación insuficiente de ciertos elementos dentro de las grabaciones de Webex. Un atacante remoto podría ejecutar código arbitrario en el sistema. Se han asignado los identificadores CVE-2020-3127 y CVE-2020-3128 para estas vulnerabilidades.
- Cisco Prime Network Registrar es vulnerable a un ataque de *Coss-site Request Forgery*. Un atacante remoto podría realizar modificaciones en la configuración del dispositivo. Se ha asignado el identificador CVE-2020-3148 para esta vulnerabilidad.
- Una vulnerabilidad en la implementación de SSL de Cisco Intelligent Proximity en Cisco Webex podría permitir a un atacante remoto, no autenticado, realizar un ataque de *Man in the middle* e interceptar el tráfico. Se ha asignado el identificador CVE-2020-3155 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Desbordamiento de búfer en Point-to-Point Protocol Daemon

Fecha de publicación: 06/03/2020

Importancia: Crítica

Recursos afectados:

Demonio pppd (*Point to Point Protocol Daemon*), desde la versión 2.4.2, hasta la 2.4.8.

Descripción:

El investigador Ilja Van Sprundel, de IOActive, ha detectado una vulnerabilidad de severidad crítica que afecta al demonio pppd. Un atacante remoto, no autenticado, podría realizar un desbordamiento de búfer y, de este modo, ejecutar código arbitrario en el sistema.

Solución:

Aplicar el último parche disponible de pppd en función de las configuraciones que se dispongan en este. Para obtener más información, consultar el apartado *Referencias*.

Detalle:

Debido a un fallo en el procesado de paquetes de *Extensible Authentication Protocol* (EAP) en el demonio pppd, un atacante remoto, no autenticado, podría realizar un desbordamiento de búfer que podría permitirle ejecutar código arbitrario en el sistema. Se ha asignado el identificador CVE-2020-8597 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Denegación de servicio en Spectrum Scale de IBM

Fecha de publicación: 09/03/2020

Importancia: Alta

Recursos afectados:

IBM Spectrum Scale, todas las versiones.

Descripción:

El investigador Honggang Ren, de Fortinet, ha reportado a IBM una vulnerabilidad de criticidad alta que afecta a todas las versiones de IBM Spectrum Sacle. Un atacante remoto podría generar una condición de denegación de servicio.

Solución:

IBM ha publicado varias actualizaciones que mitigan la vulnerabilidad en función de la versión del producto.

- IBM Spectrum Scale, desde la versión V5.0.0.0 hasta la 5.0.4.2, actualizar a la versión V5.0.4.3,
- IBM Spectrum Scale, desde la versión V4.2.0.0 hasta la 4.2.3.19, actualizar a la versión V4.2.2.20.

En caso de no poder aplicar las actualizaciones de seguridad, póngase en contacto con el servicio de atención de IBM.

Detalle:

La vulnerabilidad reside en el sistema de archivos de Spectrum Scale. Un atacante remoto podría generar una condición de servicio en los sistemas gestionados por Spectrum Scale. Se ha reservado el identificador CVE-2020-4217 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Ejecución remota de código en Desktop Central de ManageEngine

Fecha de publicación: 09/03/2020

Importancia: Crítica

Recursos afectados:

ManageEngine Desktop Central, versión 10.0.473 y anteriores.

Descripción:

Steven Seeley, de Source Incite, ha descubierto una vulnerabilidad, de severidad crítica, que permitiría a un usuario remoto tomar el control del sistema afectado.

Solución:

Actualizar el producto afectado a la versión 10.0.479.

Detalle:

Esta vulnerabilidad permitiría a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas de ManageEngine Desktop Central. No se requiere autenticación para explotar esta vulnerabilidad. El problema se debe a la falta de validación adecuada de los datos suministrados por el usuario, lo que puede dar lugar a la deserialización de los datos no fiables. Se ha asignado el identificador CVE-2020-10189 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de marzo de 2020

Fecha de publicación: 11/03/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge (basado en Chromium);
- ChakraCore;
- Internet Explorer;
- Microsoft Exchange Server;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Azure DevOps;
- Windows Defender;
- Visual Studio.;
- Open Source Software;
- Azure;
- Microsoft Dynamics;
- Microsoft Server Message Block 3.1.1 (SMBv3), en Windows 10 y Windows Server; versiones 1909 y 1903.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de marzo, consta de 114 vulnerabilidades, 26 clasificadas como críticas y 88 como importantes.

IMPORTANTE: mención especial a una vulnerabilidad de severidad crítica que afecta a SMBv3.

Solución:

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

IMPORTANTE: la vulnerabilidad con identificador CVE-2020-0796 de SMBv3 no dispone de actualización que mitigue el fallo encontrado, pero Microsoft ha publicado una serie de recomendaciones hasta la divulgación del parche:

- Deshabilitar la compresión de SMBv3 en servidores:
  - SMBv3 Server, ejecutar la siguiente línea en PowerShell, esta no previene la explotación en clientes SMB:
    - *Set-ItemProperty -Path "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParameters" DisableCompression -Type DWORD -Value 1 -Force*
  - Adicionalmente se recomienda bloquear el puerto TCP 445.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- ejecución remota de código,
- escalada de privilegios,
- denegación de servicio,
- divulgación de información,
- suplantación de identidad (*spoofing*),
- manipulación de información (*tampering*).

IMPORTANTE: Microsoft SMBv3 tiene una vulnerabilidad, identificada con el código CVE-2020-0796, a la hora de gestionar ciertas peticiones del protocolo. Un atacante remoto, no autenticado, podría ejecutar código malicioso en el equipo afectado. Esta vulnerabilidad es susceptible de aprovecharse de forma masiva.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

Actualización de seguridad de SAP de marzo de 2020

Fecha de publicación: 11/03/2020

Importancia: Crítica

Recursos afectados:

- SAP Solution Manager (User Experience Monitoring y Diagnostics Agent), versión 7.2;
- SAP Business Client, versión 6.5;
- SAP NetWeaver:
  - UDDI Server (Services Registry), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
  - AS ABAP Business Server Pages (Smart Forms) SAP_BASIS, versiones 7.00, 7.01, 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53 y 7.54;
  - Application Server Java (User Management Engine), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50.
- SAP Business Objects Business Intelligence Platform (Crystal Reports), versiones 4.1 y 4.2;
- SAP Disclosure Management, versión 10.1;
- SAP BusinessObjects Mobile (MobileBIService), versión 4.2;
- SAP MaxDB (liveCache), versiones 7.8 y 7.9;
- SAP Commerce Cloud:
  - Testweb Extension, versiones 6.6, 6.7, 1808, 1811 y 1905;
  - SmartEdit Extension, versiones 6.6, 6.7, 1808 y 1811.
- SAP ERP (EAPPGLO), versión 607;
- SAP Enable Now, versiones anteriores a 1911;
- SAP Fiori Launchpad, versiones 753 y 754;
- SAP Cloud Platform Integration para Data Services, versión 1.0;
- SAP Treasury y Risk Management (Transaction Management), versiones EA-FINSERV 600, 603, 604, 605, 606, 616, 617, 618, 800, S4CORE 101, 102, 103 y 104.

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 16 notas de seguridad de las cuales, 2 son actualizaciones de notas de seguridad publicadas con anterioridad, 3 de severidad crítica, 3 de severidad alta y 10 de severidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 4 vulnerabilidades de XSS (*Cross-Site Scripting*),
- 3 vulnerabilidades de falta de comprobación de autenticación,
- 2 vulnerabilidades de falta de comprobación,
- 1 vulnerabilidad de inyección SQL,
- 1 vulnerabilidad de ejecución remota de código (RCE),
- 1 vulnerabilidad de acceso a rutas no controlado,
- 1 vulnerabilidad de denegación de servicio (DoS),
- 5 vulnerabilidades de otro tipo.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-6207, CVE-2020-6198, CVE-2020-6203, CVE-2020-6208, CVE-2020-6209, CVE-2020-6196, CVE-2018-2450, CVE-2020-6201, CVE-2020-6205, CVE-2020-6202, CVE-2020-6199, CVE-2020-6178, CVE-2020-6210, CVE-2020-6206, CVE-2020-6204 y CVE-2020-6197.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.16

Fecha de publicación: 11/03/2020

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones:
  - desde la 1.7.0, hasta la 3.9.15;
  - desde la 3.2.0, hasta la 3.9.15;
  - desde la 3.0.0, hasta la 3.9.15;
  - desde la 2.5.0, hasta la 3.9.15;
  - desde la 3.7.0, hasta la 3.9.15.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 6 vulnerabilidades de criticidad baja en su núcleo, de los tipos SQL injection, CSRF, XSS, acceso de control incorrecto y colisión de identificadores.

Solución:

- Actualizar a la versión 3.9.16.

Detalle:

- La falta de casting de tipos en una variable de una instrucción SQL conduce a una vulnerabilidad de inyección SQL en el menú frontal de "Artículos destacados". Se ha reservado el identificador CVE-2020-10243 para esta vulnerabilidad.
- La falta de comprobación en las acciones de imagen en com_templates provoca vulnerabilidades CSRF. Se ha reservado el identificador CVE-2020-10241 para esta vulnerabilidad.
- El manejo inadecuado de los selectores de CSS en el JavaScript de Protostar y Beez3 permite los ataques mediante XSS. Se ha reservado el identificador CVE-2020-10242 para esta vulnerabilidad.
- Varias acciones en las plantillas de comunicación carecen de las comprobaciones ACL necesarias, lo que conduce a varios vectores potenciales de ataque. Se ha reservado el identificador CVE-2020-10238 para esta vulnerabilidad.
- La falta de controles de longitud en la tabla de usuarios puede llevar a la creación de usuarios con nombres de usuario y/o direcciones de correo electrónico duplicados. Se ha reservado el identificador CVE-2020-10240 para esta vulnerabilidad.
- El control de acceso incorrecto en el tipo de campo SQL de com_fields permite el acceso de usuarios que no son superadmin. Se ha reservado el identificador CVE-2020-10239 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidades en múltiples productos de Intel

Fecha de publicación: 11/03/2020

Importancia: Alta

Recursos afectados:

- Intel® Graphics Drivers, para las generaciones de procesadores Intel® desde la tercera a la décima, para Windows 7, 8.1 y 10, en versiones anteriores a 15.40.44.5107, 15.45.29.5103, 26.20.100.7584, 15.33.49.5100 y 15.36.38.5117;
- Intel® NUC e Intel® Compute Stick (consultar la versión concreta en el aviso);
- BlueZ, versiones anteriores a 5.53;
- Intel® Smart Sound Technology, en productos que tengan versiones anteriores de las siguientes:
  - 10th Generation Intel® Core™ i7 Processors, versión 3431;
  - 8th Generation Intel® Core™ Processors, versión 3349.

Descripción:

Intel ha descubierto 10 vulnerabilidades de criticidad alta, 10 medias y una baja, en múltiples productos.

Solución:

Intel recomienda ejecutar las siguientes acciones:

- actualizar Intel® Graphics Drivers para Windows a la última versión;
- actualizar Intel® NUC y Compute Stick a la última versión disponible, según está descrito en la tabla del aviso;
- actualizar BlueZ a la versión 5.53 o posterior;
- actualizar Intel Smart Sound Technology a la última versión disponible.

Detalle:

- Las vulnerabilidades de severidad alta permitirían realizar las siguientes acciones a un atacante local (salvo en CVE-2020-0556, donde el acceso es adyacente):
  - desbordamiento de búfer (CVE-2020-0504 y CVE-2020-0501);
  - control de acceso inadecuado (CVE-2020-0516 y CVE-2020-0519);
  - acceso a rutas no controlado (CVE-2020-0520);
  - comprobación de condiciones inadecuada (CVE-2020-0505);
  - restricciones inadecuadas en el búfer (CVE-2020-0530);
  - validación de datos de entrada errónea (CVE-2020-0526);
  - control de acceso inadecuado (CVE-2020-0556 y CVE-2020-0583)

Para el resto de vulnerabilidades se han reservado los identificadores: CVE-2020-0565, CVE-2020-0514, CVE-2020-0515, CVE-2020-0508, CVE-2020-0511, CVE-2020-0503, CVE-2020-0567, CVE-2020-0502, CVE-2020-0507, CVE-2020-0517 y CVE-2020-0506.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en PAN-OS de Palo Alto Networks

Fecha de publicación: 12/03/2020

Importancia: Alta

Recursos afectados:

PAN-OS, versiones anteriores a 8.1.13.

Descripción:

Palo Alto Networks ha publicado 3 vulnerabilidades, todas de severidad alta, que permitirían a un atacante local escalar privilegios y ejecutar comandos de *shell*.

Solución:

Actualizar PAN-OS a la versión 8.1.13 o posteriores.

Detalle:

- Una vulnerabilidad en la cadena de formato del demonio de registro de PAN-OS (*logd*) en Panorama, permitiría a un usuario local,

autentificado, ejecutar código arbitrario, omitiendo la restricción de acceso al *shell* y escalando los privilegios. Se ha asignado el identificador CVE-2020-1979 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de comandos de *shell* en el PAN-OS CLI permite a un usuario local, autentificado, omitir la restricción de acceso al *shell* y escalar sus privilegios. Se ha asignado el identificador CVE-2020-1980 para esta vulnerabilidad.
- Una vulnerabilidad en los nombres de archivos temporales predecibles en PAN-OS permitiría realizar una escalada local de privilegios. Se ha asignado el identificador CVE-2020-1981 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en TIBCO Spotfire Server

Fecha de publicación: 12/03/2020

Importancia: Crítica

Recursos afectados:

- TIBCO Spotfire Analytics Platform para AWS Marketplace, versiones 10.8.0 y anteriores;
- TIBCO Spotfire Server, versiones 7.11.9 y anteriores;
- TIBCO Spotfire Server, versiones 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5 y 10.3.6;
- TIBCO Spotfire Server, versiones 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0 y 10.8.0;
- Spotfire library.

Descripción:

Se ha publicado un problema en TIBCO Spotfire Server Script que podría permitir a un atacante la ejecución remota de código.

Solución:

- TIBCO Spotfire Analytics Platform para AWS Marketplace 10.8.1 o superior,
- TIBCO Spotfire Server:
  - 7.11.10 o superior,
  - 10.3.7 o superior,
  - 10.8.1 o superior.

Detalle:

La vulnerabilidad podría permitir a un atacante con permisos de escritura en la biblioteca de Spotfire, pero no con permiso del grupo "Script Author", modificar los atributos de los archivos y objetos guardados en la biblioteca de manera que el sistema los trate como confiables, haciendo que Spotfire Web Player, Analyst clients y TERR Service, ejecuten código arbitrario con los mismos privilegios que la cuenta del sistema que inició esos procesos. Se ha asignado el identificador CVE-2020-9408 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en VMware

Fecha de publicación: 13/03/2020

Importancia: Crítica

Recursos afectados:

- VMware Workstation Pro / Player (Workstation), versiones 15.x;
- VMware Fusion Pro / Fusion (Fusion), versiones 11.x;
- VMware Horizon Client para Windows, versiones 5.x y anteriores,
- VMware Remote Console para Windows (VMRC), versiones 10.x.

Descripción:

VMware ha publicado tres vulnerabilidades, una de severidad crítica y dos altas, que podrían permitir a un atacante la ejecución de código en el host, la denegación del servicio vmnetdhcp en el host, la escalada local de privilegios o ejecutar comandos como otro usuario.

Solución:

Actualizar a las siguientes versiones:

- Workstation 15.5.2,
- Fusion 11.5.2,
- Horizon Client para Windows 5.30,
- VMRC para Windows 11.0.0.

Detalle:

- La vulnerabilidad de severidad crítica:
  - VMware Workstation y Fusion contienen una vulnerabilidad de *use-after* en vmnetdhcp que podría permitir a un atacante la ejecución de código en el host del huésped o crear una condición de denegación de servicio en vmnetdhcp que se ejecuta en la máquina del host. Se ha asignado el identificador CVE-2020-3947 para esta vulnerabilidad.
- Las vulnerabilidades con severidad alta:
  - Las máquinas virtuales de Linux que se ejecutan en VMware Workstation y Fusion contienen una vulnerabilidad de escalada de privilegios local debido a permisos de archivo inadecuados en Cortado Thinprint. La explotación sólo es posible si VMware Tools está instalado en la máquina virtual (opción predeterminada en Workstation y en Fusion). Un atacante sin acceso de administrador podría aprovechar esta vulnerabilidad para escalar privilegios en la máquina virtual. Se ha asignado el identificador CVE-2020-3948 para esta vulnerabilidad.
  - En VMware Horizon Client, VMRC y Workstation para Windows, la carpeta que contiene los archivos de configuración para el servicio de arbitraje de VMware USB puede ser sobreescrita por cualquier usuario, lo cual podría permitir a un atacante ejecutar comandos como otro usuario. Se ha asignado el identificador CVE-2020-5543 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 16/03/2020

Importancia: Alta

Recursos afectados:

- Desde la versión 3.8, hasta la 3.8.1;
- Desde la versión 3.7, hasta la 3.7.4;
- Desde la versión 3.6, hasta la 3.6.8;
- Desde la versión 3.5, hasta la 3.5.10;
- Versiones anteriores sin soporte.

Descripción:

Los investigadores, Brendan Heywood y Tim Hunt, ha reportado tres vulnerabilidades, una de criticidad alta y dos bajas, que afectan a Moodle. Un atacante, remoto, podría evadir las restricciones de seguridad, revelar información o inyección de código.

Solución:

Moodle ha publicado diversas actualizaciones en función de la versión afectada:

- 3.8.2;
- 3.7.5;
- 3.6.9;
- 3.5.11.

Detalle:

La vulnerabilidad de severidad alta podría permitir a un atacante remoto utilizar las cabeceras *X-Forwarded-For* para suplantar la IP de un usuario y de este modo, evadir las comprobaciones de las direcciones IP. Se ha reservado el identificador CVE-2020-1755 para esta vulnerabilidad.

A las vulnerabilidades de severidad baja se les han reservado los identificadores CVE-2020-1754 y CVE-2020-1756.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos de VMware

Fecha de publicación: 18/03/2020

Importancia: Alta

Recursos afectados:

- VMware Workstation Pro / Player (Workstation);
- VMware Fusion Pro / Fusion (Fusion);
- VMware Remote Console para Mac (VMRC para Mac);
- VMware Horizon Client para Mac;
- VMware Horizon Client para Windows.

Descripción:

Los investigadores, Jefball de GRIMM, Dhanesh Kizhakkinan de FireEye Inc. y Rich Mirch, han reportado dos vulnerabilidades, una de severidad alta y otra baja. Un atacante local podría realizar una elevación de privilegios o generar una condición de denegación de servicio.

Solución:

VMware ha publicado una serie de actualizaciones que mitigan las vulnerabilidades.

- Fusion, versión 11.X, actualizar a la versión 11.5.2;
- VMRC para Mac, versiones 11.X y anteriores, actualizara la versión 11.0.1;
- Horizon Client para Mac, versiones 5.X y anteriores, actualizar a la versión 5.4.0.
- Workstation para Windows, versión 15.X, actualizar a la versión 15.5.2 (pro y player);
- Horizon Client para Windows, versiones 5.X y anteriores, actualizar a la versión 5.4.0.

Detalle:

- La vulnerabilidad de criticidad alta, que afecta a VMware Fusion, VMRC para Mac y Horizon Client para Mac, es debida a un uso indebido de los binarios *setuid*. Un atacante local podría realizar una elevación de privilegios y obtener privilegios de *root* en el sistema afectado. Se ha asignado el identificador CVE-2020-3950 para esta vulnerabilidad.
- A la vulnerabilidad de criticidad baja se le ha asignado el identificador CVE-2020-3951.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 20/03/2020

Importancia: Alta

Recursos afectados:

Estas vulnerabilidades afectan a los siguientes productos Cisco si están ejecutando una versión del software Cisco SD-WAN Solution anterior a la 19.2.2:

- vBond Orchestrator Software,
- vEdge 100 Series Routers,
- vEdge 1000 Series Routers,
- vEdge 2000 Series Routers,
- vEdge 5000 Series Routers,
- vEdge Cloud Router Platform,
- vManage Network Management (Software y System),
- vSmart Controller Software.

Descripción:

Orange Group ha detectado 3 vulnerabilidades de criticidad alta que afectan a múltiples productos. Un atacante local, no autenticado, podría realizar un desbordamiento de búfer, elevar los privilegios a nivel *root* y ejecutar comandos arbitrarios en el dispositivo afectado.

Solución:

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

Detalle:

- Un atacante local, no autenticado, podría causar un desbordamiento de búfer mediante el envío de tráfico, especialmente diseñado, al dispositivo afectado, aprovechando una validación insuficiente de datos de entrada. Se ha reservado el identificador CVE-2020-3264 para esta vulnerabilidad.
- Un atacante local, no autenticado, podría realizar una elevación de privilegios de root mediante el envío de una petición, especialmente diseñada, al sistema operativo afectado, aprovechando una validación insuficiente de datos de entrada. Se ha reservado el identificador CVE-2020-3265 para esta vulnerabilidad.
- Un atacante local, no autenticado, podría realizar una inyección de comandos arbitrarios que serían ejecutados con privilegios de root mediante el envío de datos, especialmente diseñados, a la utilidad CLI, aprovechando una validación insuficiente de datos de entrada. Se ha reservado el identificador CVE-2020-3266 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Liferay Portal

Fecha de publicación: 20/03/2020

Importancia: Crítica

Recursos afectados:

- Liferay Portal, versión 6.2.5 y anteriores;
- Liferay Portal, versión 7.0.0 y anteriores.

Descripción:

Liferay ha detectado dos vulnerabilidades de severidad crítica que afectan a sus productos. Un atacante remoto, autenticado, podría ejecutar código arbitrario o revelar información.

Solución:

- Liferay Portal 6.2.5, aplicar el parche de seguridad disponible en GitHub.
- Liferay Portal 7.0.0, no hay parche disponible. Desde Liferay recomiendan actualizar a la versión Liferay Portal 7.0.1 o posterior.

Detalle:

- Una vulnerabilidad existente en las plantillas DDM en Liferay Portal 6.2.5 y anteriores, podría permitir a un atacante remoto, autenticado, con permisos de creación y edición de plantillas, visualizar cualquier archivo legible por el proceso JVM del portal.
- Una vulnerabilidad existente en la plantilla DDM en Liferay Portal 7.0.0 y anteriores, podría permitir a un atacante remoto, autenticado, con permisos de edición y creación de plantillas, generar plantillas que pueden ejecutar código arbitrario.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el core de Drupal

Fecha de publicación: 20/03/2020

Importancia: Media

Recursos afectados:

- 8.8.x;
- 8.7.x.

Descripción:

Una biblioteca de terceros utilizada por el proyecto Drupal ha liberado una mejora de seguridad necesaria para proteger algunas de sus configuraciones.

Solución:

Actualizar a las versiones 8.8.4 o 8.7.12, donde se incluye la actualización 4.14 de CKEditor.

Para mitigar la vulnerabilidad, el módulo CKEditor también se puede deshabilitar hasta que se actualice el sitio.

Detalle:

Si Drupal está configurado para permitir el uso del CKEditor WYSIWYG, un atacante podría llevar a cabo ataques XSS contra otros usuarios, incluyendo administradores, cuando varias personas puedan editar los contenidos.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de creación de objetos no segura en Ruby

Fecha de publicación: 20/03/2020

Importancia: Alta

Recursos afectados:

JSON gem, versión 2.2.0 o anteriores.

Descripción:

Jeremy Evans ha descubierto una vulnerabilidad de severidad alta en la gema JSON de Ruby, que permitiría la creación de objetos arbitrarios en el sistema afectado.

Solución:

Actualizar la gema JSON a la versión 2.3.0 o posterior.

Detalle:

Al analizar ciertos documentos JSON, la gema JSON (incluyendo la que viene con Ruby) puede ser obligada a crear objetos arbitrarios en el sistema. Se ha reservado el identificador CVE-2020-10663 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en PHP 7

Fecha de publicación: 20/03/2020

Importancia: Alta

Recursos afectados:

PHP 7, todas las versiones anteriores a la versión 7.4.4.

Descripción:

PHP ha detectado una vulnerabilidad de criticidad alta. Un atacante remoto podría obtener información sensible o realizar inyección de datos.

Solución:

Actualizar PHP 7 a la versión 7.4.4 o posterior.

Detalle:

La función *get_headers()* trunca silenciosamente a partir de la introducción de un byte nulo en la URL. Un atacante remoto podría obtener información sensible o realizar inyección de datos. Se ha reservado el identificador CVE-2020-7066 para esta vulnerabilidad.

Etiquetas: Actualización, PHP, Vulnerabilidad

Redireccionamiento abierto en IBM Jazz for Service Management

Fecha de publicación: 23/03/2020

Importancia: Alta

Recursos afectados:

IBM Jazz for Service Management (JazzSM), versión 1.1.3.

Descripción:

IBM Jazz for Service Management contiene una vulnerabilidad, de severidad alta, de tipo redireccionamiento abierto.

Solución:

Instalar el parche 1.1.3-TIV-JazzSM-multi-FP006.

Detalle:

IBM Jazz for Service Management es vulnerable a redireccionamiento abierto, que se origina cuando una aplicación incorpora datos gestionados por el usuario que podrían contener un redireccionamiento malicioso.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidades de ejecución remota de código en Microsoft Windows

Fecha de publicación: 24/03/2020

Importancia: Crítica

Recursos afectados:

- Windows 10, todas las versiones;
- Windows 8.1, arquitectura de 32 y 64 bits;
- Windows RT 8.1;
- Windows 7 Service pack 1, arquitectura de 32 y 64 bits;
- Windows Server 2008 Service pack 2 y Server Core installation, arquitectura de 32 y 64 bits;
- Windows Server 2012 y Server Core instalation;
- Windows Server 2012 R2 y Server Core instalation;
- Windows Server 2016 y Server Core instalation;
- Windows Server 2019 y Server Core installation.

Descripción:

Microsoft ha detectado dos vulnerabilidades de severidad crítica. Un atacante remoto podría realizar una ejecución código en el sistema.

Solución:

Actualmente no hay ningún parche que mitigue las vulnerabilidades. Microsoft ha publicado una serie de recomendaciones:

- Deshabilitar el panel de previsualización y el panel de detalles en Windows Explorer;
- Deshabilitar el servicio WebClient;
- Renombrar ATMFD.DLL. Esta librería no se encuentra en las instalaciones de Windows 10, desde la versión Windows 10 1709.

Puede obtener más información sobre cómo llevar a cabo estas recomendaciones, según su producto afectado, en la sección *Referencias*.

Detalle:

Existen dos vulnerabilidades en la librería *Windows Adobe Type Manager Library* de Microsoft Windows, debido a un manejo incorrecto de la fuente multimaestro *Adobe Type 1 PostScritp format* específicamente creada.

Etiquetas: Microsoft, Vulnerabilidad, Windows

Vulnerabilidades de inyección SQL en phpMyAdmin

Fecha de publicación: 24/03/2020

Importancia: Alta

Recursos afectados:

phpMyAdmin, versiones 4.9.x anteriores a 4.9.5, y versiones 5.0.x anteriores a 5.0.2.

Descripción:

Los investigadores hoangn144_VCS, bluebird y Yutaka WATANABE, han reportado 3 vulnerabilidades, 2 de severidad alta y una media, todas de inyección SQL.

Solución:

Actualizar a las versiones 4.9.5 o 5.0.2 o posteriores. También se pueden aplicar los siguientes parches:

- CVE-2020-10804:
  - 89fbcd7c39e6b3979cdb2f64aa4cd5f4db27eaad,
  - 3258978c38bee8cb4b99f249dffac9c8aaea2d80.
- CVE-2020-10802: a8acd7a42cf743186528b0453f90aaa32bfefabe.
- CVE-2020-10803:
  - 2489837213b90664aceebe4c9ac641bf167b8a97,
  - 46a7aa7cd4ff2be0eeb23721fbf71567bebe69a5,
  - 6b9b2601d8af916659cde8aefd3a6eaadd10284a.

Detalle:

- Un atacante, con acceso al servidor, podría aprovecharse de una vulnerabilidad de inyección SQL para crear un nombre de usuario, especialmente diseñado, y engañar a la víctima para que realice acciones específicas con esa cuenta de usuario. Además, podría generar errores en el servidor para los usuarios con ciertos caracteres que tratan de cambiar sus contraseñas de MySQL. Se ha asignado el identificador CVE-2020-10804 para esta vulnerabilidad.
- Se ha descubierto una vulnerabilidad de inyección SQL en la que no se escapan correctamente ciertos parámetros al generar determinadas consultas para acciones de búsqueda dentro de phpMyAdmin, que permitiría a un atacante generar bases de datos o nombres de tablas especialmente diseñadas. Se ha asignado el identificador CVE-2020-10802 para esta vulnerabilidad.

Se ha asignado el identificador CVE-2020-10803 para la vulnerabilidad de severidad media.

Etiquetas: Actualización, PHP, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en Dell EMC iDRAC

Fecha de publicación: 25/03/2020

Importancia: Alta

Recursos afectados:

- Dell EMC iDRAC7, versiones anteriores a 2.65.65.65;
- Dell EMC iDRAC8, versiones anteriores a 2.70.70.70;
- Dell EMC iDRAC9, versiones anteriores a 4.00.00.00.

Descripción:

Varias versiones de Dell EMC iDRAC contienen una vulnerabilidad, clasificada con severidad alta, de tipo desbordamiento de búfer.

Solución:

Actualizar los productos afectados a las siguientes versiones, disponibles desde el centro de descargas del fabricante:

- Dell EMC iDRAC7, versión 2.65.65.65;
- Dell EMC iDRAC8, versión 2.70.70.70;
- Dell EMC iDRAC9, versión 4.00.00.00.

Detalle:

Una vulnerabilidad de desbordamiento de búfer basado en pila (*stack*), que afecta a varias versiones de Dell EMC iDRAC, permitiría a un atacante remoto, no autenticado, bloquear el proceso afectado o ejecutar código arbitrario en el sistema enviando datos de entrada especialmente diseñados. Se ha reservado el identificador CVE-2020-5344 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 26/03/2020

Importancia: Alta

Recursos afectados:

- Jenkins LTS, versión 2.204.5 y anteriores;
- Jenkins weekly, versión 2.227 y anteriores.

Descripción:

Jenkins ha detectado 4 vulnerabilidades, una de criticidad alta y 3 medias, que afectan a su *core* y permitirían realizar ataques de tipo CSRF (*Cross-Site Request Forgery*) y XSS (*Cross-Site Scripting*) persistente.

Solución:

- Jenkins LTS, actualizar a la versión 2.204.6 o 2.222.1;
- Jenkins weekly, actualizar a la versión 2.228.

Detalle:

- Un punto de extensión en Jenkins permite desactivar selectivamente la protección contra ataques de tipo CSRF para URL específicas, ya que recibe una representación diferente de la ruta de la URL de la que el *framework* para aplicaciones web Stapler utiliza para realizar solicitudes de envío. Se ha asignado el identificador CVE-2020-2160 para esta vulnerabilidad.
- Para las vulnerabilidades de severidad media, se han asignado los identificadores: CVE-2020-2161, CVE-2020-2162 y CVE-2020-2163.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en WebSphere Application Server de IBM

Fecha de publicación: 26/03/2020

Importancia: Alta

Recursos afectados:

WebSphere Application Server, versiones 7.0, 8.0, 8.5 y 9.0.

Descripción:

IBM ha publicado una vulnerabilidad en WebSphere Application Server que podría permitir a un atacante la escalada de privilegios.

Solución:

Aplicar las siguientes actualizaciones en función de la versión:

- Desde la V9.0.0.0 hasta la 9.0.5.3:
  - Actualizar según los requisitos del interim fix y luego aplicar el Interim Fix PH21511, o aplicar el Fix Pack 9.0.5.4 o posterior (disponible en el segundo cuatrimestre de 2020).
- Desde la V8.5.0.0 hasta la 8.5.5.17:
  - Actualizar según los requisitos del interim fix y luego aplicar el Interim Fix PH21511, o aplicar el Fix Pack 8.5.5.18 o posterior (disponible en el tercer cuatrimestre de 2020).
- Desde la V8.0.0.0 hasta 8.0.0.15:
  - Actualizar a la 8.0.0.15 y luego aplicar el Interim Fix PH21511.
- Desde la V7.0.0.0 hasta la 7.0.0.45:
  - Actualizar a la 7.0.0.45 y luego aplicar el Interim Fix PH21511.

Detalle:

Una vulnerabilidad en IBM WebSphere Application Server podría permitir a un atacante la escalada de privilegios cuando se utiliza la autenticación basada en *tokens* en una solicitud de administración sobre el conector SOAP. Se ha reservado el identificador CVE-2020-4276 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos F5

Fecha de publicación: 27/03/2020

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:
  - 15.0.0 - 15.0.1 y 15.1.0.1;
  - 14.0.0 - 14.1.2;
  - 13.1.0 - 13.1.3;
  - 12.1.0 - 12.1.5;
  - 11.5.2 - 11.6.5.
- BIG-IQ Centralized Management, versiones:
  - 7.0.0;
  - 6.0.0 - 6.1.0;
  - 5.2.0 - 5.4.0.

Descripción:

Se han publicado múltiples vulnerabilidades en productos F5 que podrían permitir a un atacante realizar una denegación de servicio, una escalada de privilegios o el cierre inesperado de Traffic Management Microkernel (TMM).

Solución:

Aplicar la actualización correspondiente en función de la versión.

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 15.1.0;
  - 15.1.0.2;
  - 15.0.1.1;
  - 14.1.2.3;
  - 13.1.3.2;
  - 12.1.5.1.
- BIG-IQ Centralized Management, versiones:
  - Actualmente no dispone de actualización.

Detalle:

- Las peticiones HTTP no reveladas podrían provocar una denegación de servicio (DoS). Se requiere un perfil HTTP y cualquier módulo BIG-IP que utilice el perfil HTTP está afectado. Se ha reservado el identificador CVE-2016-5857 para esta vulnerabilidad.
- Los usuarios con roles no administrativos, por ejemplo "Invitado" o "Administrador de Recursos", con acceso a TMOS Shell (tmsh), podrían ejecutar comandos arbitrarios con altos privilegios, usando un comando *tmsh* especialmente diseñado. Se ha reservado el identificador CVE-2020-5858 para esta vulnerabilidad.
- Un atacante, mediante mensajes HTTP/3, especialmente diseñados, podría provocar que el TMM se reinicie y falle temporalmente al procesar el tráfico en hosts BIG-IP con el perfil HTTP/3 QUIC configurado. Las configuraciones de alta disponibilidad (HA) fallarán sobre el *host* de reserva. Se ha reservado el identificador CVE-2020-5859 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Escalada de privilegios en Apache Traffic Server

Fecha de publicación: 27/03/2020

Importancia: Crítica

Recursos afectados:

Apache Traffic Server (ATS), versiones:

- 6.0.0 - 6.2.3;

- 7.0.0 - 7.1.8;
- 8.0.0 - 8.0.5.

Descripción:

ZeddYu Lu ha reportado múltiples vulnerabilidades en Apache Traffic Server que podrían permitir a un atacante remoto la escalada de privilegios.

Solución:

Actualizar a la versión correspondiente, desde el centro de descargas de ATS:

- Para versiones 6.x:
  - 7.1.9, 8.0.6 o posteriores.
- Para versiones 7.x:
  - 7.1.9 o posteriores.
- Para versiones 8.x:
  - 8.0.6 o posteriores.

Detalle:

Las vulnerabilidades publicadas, del tipo ataque de tráfico no autorizado y codificación fragmentada, podrían permitir a un atacante remoto la escalada de privilegios debido a una interpretación inadecuada de las solicitudes HTTP. Se han asignado los identificadores CVE-2020-1944, CVE-2019-17565 y CVE-2019-17559 para estas vulnerabilidades.

Etiquetas: Actualización, Apache, Windows

Fallos de Cross Site Scripting (XSS) encontrados en el software Tiki-Wiki CMS

Fecha de publicación: 30/03/2020

Importancia: Media

Recursos afectados:

Tiki Wiki CMS, versión 20.0 y anteriores.

Descripción:

INCIBE ha coordinado la publicación de una vulnerabilidad en el gestor de contenidos Tiki Wiki, descubierta por Pablo Sebastián Arias Rodríguez, Rubén Barberà Pérez y Jorge Alberto Palma Reyes de S2Grupo en el CSIRT-CV. Cuenta con un agradecimiento especial al equipo del CSIRT-CV (https://www.csirtcv.gva.es) compuesto por: Lourdes Herrero, Maite Moreno, José Vila, Adrián Antón, Adrián Capdevila, Aurora Villegas, Eva Lleonart, Fernando Cózar, Javier García, Manuel Rosa, Mario Ortiz, Mayte Aranda, Oscar Martínez, Sergio Hernández y Yolanda Olmedo que descubrieron un fallo XSS en el software Tiki-Wiki CMS

Se ha asignado el código CVE-2020-8966 a esta vulnerabilidad. Se ha calculado una puntuación base de 6,5 según CVSS v3; siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:W/RC:C/CR:H/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:N/MA:N

Solución:

Actualizar a la versión 21.0

Detalle:

Algunas páginas php reciben información de un componente ascendente, pero no neutraliza o neutraliza incorrectamente caracteres especiales como "< ", " >", y "&". Estos caracteres podrían interpretarse como elementos de secuencias de comandos web cuando se envían a un componente descendente que procesa páginas web.

CWE-80: Neutralización incorrecta de etiquetas HTML relacionadas con scripts en una página web (XSS básico)

Línea temporal
27/11/2019 ? Descubrimiento de los investigadores.
04/02/2020 ? Investigadores contactan con INCIBE.
21/02/2020 ? Tiki-Wiki Security Team confirma la vulnerabilidad a INCIBE.
28/02/2020 ? El desarrollador confirma que se han publicado una nueva versión del software y el parche corrector. INCIBE, los investigadores y el desarrollador analizan la solución y acuerdan divulgar el aviso el 31 de marzo.
31/03/2020 ? El aviso ha sido publicado por INCIBE.

Todos los avisos incluidos en INCIBE se proporcionan "tal cual" con fines, únicamente, informativos. INCIBE no ofrece garantías de ningún tipo con respecto a la información contenida en el mismo. INCIBE no respalda ningún producto o servicio comercial, mencionado en este aviso.

Si tiene información sobre este aviso, comuníquese con INCIBE como se indica en la divulgación de vulnerabilidades.

Etiquetas: 0day, CMS, CNA, Vulnerabilidad

Múltiples vulnerabilidades en Vertiv Avocent UMG-4000

Fecha de publicación: 31/03/2020

Importancia: Alta

Recursos afectados:

Vertiv Avocent UMG-4000, versión 4.2.1.19.

Descripción:

El producto Avocent UMG-4000 de Vertiv contiene 3 vulnerabilidades, una de severidad alta y 2 de severidad media, de tipo inyección de comandos y XSS persistente.

Solución:

- Los usuarios que no usen la plataforma *Trellis* deben instalar la versión de *firmware* 4.2.2.21 o superior.
- Los usuarios que emplean *Trellis*, versiones desde 5.0.2 hasta 5.0.6, ejecutando la versión de *firmware* 4.2.0.23, deben aplicar el parche correspondiente.
- Los usuarios que utilizan *Tellis* en la versión 5.0.6 o superiores, deben instalar la versión de *firmware* 4.3.0.23.

Detalle:

- La interfaz web del producto afectado es vulnerable a una inyección de comandos porque la aplicación neutraliza incorrectamente la sintaxis del código antes de ejecutarse. Dado que todos los comandos de la aplicación web se ejecutan como *root*, esto podría permitir a un atacante remoto, autentificado, con una cuenta de administrador, ejecutar comandos arbitrarios. Se ha asignado el identificador CVE-2019-9507 para esta vulnerabilidad.

Para las vulnerabilidades de severidad media, se han asignado los identificadores CVE-2019-9508 y CVE-2019-9509.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Spectrum Protect Plus de IBM

Fecha de publicación: 31/03/2020

Importancia: Alta

Recursos afectados:

IBM Spectrum Protect Plus, versiones desde la 10.1.0 a la 10.1.5.

Descripción:

Se han publicado vulnerabilidades en IBM Spectrum Protect Plus del tipo evasión de autenticación, eliminación arbitraria de directorios e inyección de comandos, que podrían permitir a un atacante remoto ejecutar código arbitrario en el sistema.

Solución:

Actualizar a la versión 10.1.5.2199.

Detalle:

- La existencia de credenciales embebidas, como contraseñas y llaves criptográficas, podría permitir a un atacante ejecutar código arbitrario en el sistema. Se ha reservado el identificador CVE-2020-4208 para esta vulnerabilidad.
- La validación inadecuada de los datos introducidos por el usuario podría permitir a un atacante remoto la eliminación arbitraria de directorios. Se ha reservado el identificador CVE-2020-4214 para esta vulnerabilidad.
- La validación inadecuada de los datos introducidos por el usuario podría permitir a un atacante remoto ejecutar comandos arbitrarios en el sistema con permisos de *root*. Se ha reservado el identificador CVE-2020-4206 para esta vulnerabilidad.
- El envío de una petición especialmente diseñada podría permitir a un atacante remoto, no autenticado, ejecutar comandos arbitrarios en el sistema. Se han reservado los identificadores CVE-2020-4241y CVE-2020-4242 para estas vulnerabilidades.

Etiquetas: Actualización, IBM, Vulnerabilidad