Boletín de septiembre de 2019

Avisos Técnicos

Evasión del directorio compartido en Samba

Fecha de publicación: 04/09/2019

Importancia: Alta

Recursos afectados:

- Samba, versiones desde la 4.9.0 hasta la 4.9.12;
- Samba, versiones desde la 4.10.0 hasta la 4.10.7.

Descripción:

El investigador de seguridad Stefan Metzmacher de SerNet, en colaboración con el equipo de Samba, ha detectado una vulnerabilidad de criticidad alta. Un atacante, autenticado, podría realizar una evasión del directorio fuera del directorio compartido.

Solución:

- Samba 4.9.X: aplicar el parche o actualizar a la versión 4.9.12;
- Samba 4.10.X: aplicar el parche o actualizar a la versión 4.10.7.

Para versiones anteriores de Samba, se irán publicando actualizaciones en el centro de descargas de Samba.

Se aconseja a los administradores de Samba que actualicen a estas versiones o que apliquen el parche lo antes posible.

Detalle:

La vulnerabilidad se debe a algunos parámetros en el archivo de configuración smb.conf. Un atacante, autenticado, podría realizar una evasión del directorio fuera del directorio compartido. Se ha asignado el identificador CVE-2019-10197 para esta vulnerabilidad.

Etiquetas: Actualización, Samba, Vulnerabilidad

Múltiples vulnerabilidades de ejecución remota de código en Aruba Mobility Controllers

Fecha de publicación: 04/09/2019

Importancia: Alta

Recursos afectados:

Aruba Mobility Controllers con las siguientes versiones de firmware:

- ArubaOS 6.x, anterior a la 6.4.4.21;
- ArubaOS 6.5.x, anterior a la 6.5.4.13;
- ArubaOS 8.x, anterior a la 8.2.2.6;
- ArubaOS 8.3.0.x, anterior a la 8.3.0.7;
- ArubaOS 8.4.0.x, anterior a la 8.4.0.3.

Descripción:

Aruba ha publicado vulnerabilidades presentes en algunas versiones que se ejecutan en Aruba Mobility Controllers y que podrían permitir a un atacante ejecutar código arbitrario en el sistema operativo subyacente con todos los privilegios del sistema.

Solución:

Aplicar las siguientes actualizaciones en función de la versión afectada:

- ArubaOS 6.4.4.21,
- ArubaOS 6.5.4.13,
- ArubaOS 8.2.2.6,
- ArubaOS 8.3.0.7,
- ArubaOS 8.4.0.3,
- ArubaOS 8.5.0.0.

Detalle:

- El componente *network-listener* presenta una vulnerabilidad de ejecución remota de código en algunas versiones de ArubaOS. Un atacante, con capacidad para transferir tráfico IP especialmente diseñado a un controlador de movilidad, aprovechando el protocolo PAPI (UDP 8211), podría causar un fallo en el proceso o ejecutar código arbitrario en el sistema operativo subyaente con todos los privilegios del sistema. Se ha reservado el identificador CVE-2018-7081 para esta vulnerabilidad.
- Algunos componentes web del software ArubaOS son vulnerables a inyección CRLF y a Cross-Site Scripting (XSS) reflejado. Un atacante podría enviar ciertos parámetros de URL para explotar esta vulnerabilidad. Se ha reservado el identificador CVE-2019-5314 para esta vulnerabilidad.
- La vulnerabilidad de inyección de comandos presente en la interfaz de gestión web de ArubaOS podría permitir a un atacante autenticado, ejecutar comandos arbitrarios en el sistema operativo subyacente. Un administrador malicioso podría utilizar esta capacidad para instalar puertas traseras o cambiar la configuración del sistema de manera que no quede registro. Esta vulnerabilidad solo afecta a ArubaOS 8.x. Se ha reservado el identificador CVE-2019-5315 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 05/09/2019

Importancia: Alta

Recursos afectados:

- Cisco IND (Industrial Network Director), versiones anteriores a 1.6.0 si tienen los servicios *plug-and-play* habilitados.
- Cisco Webex Teams para Windows, versiones anteriores a 3.0.12427.0.

Descripción:

Cisco ha detectado dos vulnerabilidades que podrían permitir a un atacante remoto, sin autenticación, acceder a información sensible o para ejecutar comandos arbitrarios en el sistema afectado.

Solución:

Actualizar a Cisco IND 1.6.0 o posteriores, y a Cisco Webex Teams 3.0.12427.0 o posteriores, ambas disponibles desde el centro de descarga de Cisco.

Detalle:

- Las restricciones de acceso inapropiadas en la interfaz de administración web en el componente de los servicios de *plug-and-play* de Cisco IND, podrían permitir a un atacante remoto, no autenticado, acceder a información sensible en el dispositivo afectado. Se ha asignado el identificador CVE-2019-1976 para esta vulnerabilidad.
- Las restricciones inapropiadas en la funcionalidad del software de registro de credenciales de Cisco Webex Teams, utilizada por la aplicación en sistemas operativos Windows, podrían permitir a un atacante remoto, no autenticado, ejecutar comandos arbitrarios en el sistema afectado. Se ha asignado el identificador CVE-2019-1939 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad en Data Protection Central Authentication de Dell EMC

Fecha de publicación: 05/09/2019

Importancia: Alta

Recursos afectados:

- Dell EMC Data Protection Central 1.0,
- Dell EMC Data Protection Central 1.0.1,
- Dell EMC Data Protection Central 18.1,
- Dell EMC Data Protection Central 18.2,
- Dell EMC Data Protection Central 19.1.

Descripción:

Dell EMC Data Protection Central presenta una vulnerabilidad de autenticación que podría permitir a un atacante comprometer el sistema afectado.

Solución:

- Actualizar a Dell EMC Data Protection Central versiones 18.2.1 y 19.1.1.

Detalle:

Una vulnerabilidad del tipo cadena de confianza del certificado inadecuada podría permitir a un atacante remoto, no autenticado, obtener un certificado firmado por CA de Data Protection Central para poder hacerse pasar por un sistema válido y comprometer la integridad de los datos. Se ha reservado el identificador CVE-2019-3762 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad 5.2.3 para WordPress

Fecha de publicación: 05/09/2019

Importancia: Alta

Recursos afectados:

WordPress, versiones 5.2.2 y anteriores.

Descripción:

Más de 62 investigadores han colaborado en la identificación de diversas vulnerabilidades, corregidas en esta versión. Se incluyen 29 correcciones y mejoras, además de una serie de correcciones de seguridad.

Solución:

Ha sido publicada la versión 5.2.3 del gestor de contenidos WordPress para solucionar dichas vulnerabilidades, disponible desde su página de descarga.

Detalle:

Las correcciones de seguridad solucionan las siguientes vulnerabilidades:

- *Cross-Site Scripting* (XSS) en las previsualizaciones de las publicaciones de los colaboradores, en los comentarios almacenados, en las previsualizaciones de códigos abreviados y por un problema al sanear una URL.
- Redirección abierta al realizar la validación y al sanear una URL.
- XSS reflejado durante la subida de contenido multimedia y en el cuadro de mandos.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 05/09/2019

Importancia: Alta

Recursos afectados:

- Los dispositivos afectados son:
  - D3600, ejecutando versiones de firmware anteriores a la versión 1.0.0.76;
  - D6000, ejecutando versiones de firmware anteriores a la versión 1.0.0.76;
  - D6220, ejecutando versiones de firmware anteriores a la versión 1.0.0.40;
  - D6220, ejecutando versiones de firmware anteriores a la versión 1.0.0.44;
  - D6400, ejecutando versiones de firmware anteriores a la versión 1.0.0.78;
  - D7000v2, ejecutando versiones de firmware anteriores a la versión 1.0.0.51;
  - D8500, ejecutando versiones de firmware anteriores a la versión 1.0.3.39;
  - D8500, ejecutando versiones de firmware anteriores a la versión 1.0.3.42;
  - DGN2200v4, ejecutando versiones de firmware anteriores a la versión 1.0.0.110;
  - DGND2200Bv4, ejecutando versiones de firmware anteriores a la versión 1.0.0.110;
  - EX3700, ejecutando versiones de firmware anteriores a la versión 1.0.0.70;
  - EX3800, ejecutando versiones de firmware anteriores a la versión 1.0.0.70;
  - EX6000, ejecutando versiones de firmware anteriores a la versión 1.0.0.30;
  - EX6100, ejecutando versiones de firmware anteriores a la versión 1.0.2.22;
  - EX6100, ejecutando versiones de firmware anteriores a la versión 1.0.2.24;
  - EX6120, ejecutando versiones de firmware anteriores a la versión 1.0.0.40;
  - EX6130, ejecutando versiones de firmware anteriores a la versión 1.0.0.22;
  - EX6150v1, ejecutando versiones de firmware anteriores a la versión 1.0.0.42;
  - EX6200, ejecutando versiones de firmware anteriores a la versión 1.0.3.88;
  - EX7000, ejecutando versiones de firmware anteriores a la versión 1.0.0.66;
  - JNDR3000, ejecutando versiones de firmware anteriores a la versión 1.0.0.22;
  - R6250, ejecutando versiones de firmware anteriores a la versión 1.0.4.26;
  - R6300v2, ejecutando versiones de firmware anteriores a la versión 1.0.4.18;
  - R6300v2, ejecutando versiones de firmware anteriores a la versión 1.0.4.22;
  - R6300v2, ejecutando versiones de firmware anteriores a la versión 1.0.4.28;
  - R6400, ejecutando versiones de firmware anteriores a la versión 1.0.1.24;
  - R6400, ejecutando versiones de firmware anteriores a la versión 1.0.1.36;
  - R6400v2, ejecutando versiones de firmware anteriores a la versión 1.0.2.32;
  - R6400v2, ejecutando versiones de firmware anteriores a la versión 1.0.2.52;
  - R6700, ejecutando versiones de firmware anteriores a la versión 1.0.1.22;
  - R6700, ejecutando versiones de firmware anteriores a la versión 1.0.1.44;
  - R6700, ejecutando versiones de firmware anteriores a la versión 1.0.1.46;
  - R6700v3, ejecutando versiones de firmware anteriores a la versión 1.0.2.32;
  - R6900, ejecutando versiones de firmware anteriores a la versión 1.0.1.22;
  - R6900, ejecutando versiones de firmware anteriores a la versión 1.0.1.44;
  - R6900, ejecutando versiones de firmware anteriores a la versión 1.0.1.46;
  - R6900P, ejecutando versiones de firmware anteriores a la versión 1.0.0.56;
  - R6900P, ejecutando versiones de firmware anteriores a la versión 1.3.1.26;
  - R6900P, ejecutando versiones de firmware anteriores a la versión 1.3.1.64;
  - R7000, ejecutando versiones de firmware anteriores a la versión 1.0.9.28;
  - R7000, ejecutando versiones de firmware anteriores a la versión 1.0.9.6;
  - R7000P, ejecutando versiones de firmware anteriores a la versión 1.0.0.56;
  - R7000P, ejecutando versiones de firmware anteriores a la versión 1.3.1.26;
  - R7000P, ejecutando versiones de firmware anteriores a la versión 1.3.1.64;
  - R7100LG, ejecutando versiones de firmware anteriores a la versión 1.0.0.42;
  - R7100LG, ejecutando versiones de firmware anteriores a la versión 1.0.0.46;

- R7300DST, ejecutando versiones de firmware anteriores a la versión 1.0.0.54;
- R7300DST, ejecutando versiones de firmware anteriores a la versión 1.0.0.62;
- R7300DST, ejecutando versiones de firmware anteriores a la versión 1.0.0.68;
- R7800, ejecutando versiones de firmware anteriores a la versión 1.0.2.60;
- R7900, ejecutando versiones de firmware anteriores a la versión 1.0.1.26;
- R7900, ejecutando versiones de firmware anteriores a la versión 1.0.2.10;
- R7900, ejecutando versiones de firmware anteriores a la versión 1.0.2.16;
- R7900P, ejecutando versiones de firmware anteriores a la versión 1.3.0.10;
- R7900P, ejecutando versiones de firmware anteriores a la versión 1.4.1.42;
- R8000, ejecutando versiones de firmware anteriores a la versión 1.0.4.12;
- R8000, ejecutando versiones de firmware anteriores a la versión 1.0.4.18;
- R8000P, ejecutando versiones de firmware anteriores a la versión 1.3.0.10;
- R8000P, ejecutando versiones de firmware anteriores a la versión 1.4.1.42;
- R8300, ejecutando versiones de firmware anteriores a la versión 1.0.2.106;
- R8300, ejecutando versiones de firmware anteriores a la versión 1.0.2.116;
- R8300, ejecutando versiones de firmware anteriores a la versión 1.0.2.122;
- R8500, ejecutando versiones de firmware anteriores a la versión 1.0.2.106;
- R8500, ejecutando versiones de firmware anteriores a la versión 1.0.2.116;
- R8500, ejecutando versiones de firmware anteriores a la versión 1.0.2.122;
- WN2500RPv2, ejecutando versiones de firmware anteriores a la versión 1.0.1.54;
- WNDR3400v3, ejecutando versiones de firmware anteriores a la versión 1.0.1.18;
- WNDR3400v3, ejecutando versiones de firmware anteriores a la versión 1.0.1.22;
- WNDR4500v2, ejecutando versiones de firmware anteriores a la versión 1.0.0.68;
- WNR3500Lv2, ejecutando versiones de firmware anteriores a la versión 1.2.0.46;
- WNR3500Lv2, ejecutando versiones de firmware anteriores a la versión 1.2.0.48;
- WNR3500Lv2, ejecutando versiones de firmware anteriores a la versión 1.2.0.54;
- XR500, ejecutando versiones de firmware anteriores a la versión 2.3.2.32.

Descripción:

Netgear ha detectado 10 vulnerabilidades de criticidad alta que afectan a múltiples productos.

Solución:

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

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades descritas en este aviso podría llegar a realizar alguna de las siguientes acciones:

- inyección SQL;
- desbordamiento de búfer;
- inyección de comandos.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 06/09/2019

Importancia: Crítica

Recursos afectados:

- GS105Ev2, ejecutando versiones de firmware anteriores a la versión 1.6.0.4;
- GS105PE, ejecutando versiones de firmware anteriores a la versión 1.6.0.4;
- GS408EPP, ejecutando versiones de firmware anteriores a la versión 1.0.0.15;
- GS728TPPv2, ejecutando versiones de firmware anteriores a la versión 6.0.0.48;
- GS728TPv2, ejecutando versiones de firmware anteriores a la versión 6.0.0.48;
- GS750E, ejecutando versiones de firmware anteriores a la versión 1.0.1.4;
- GS752TPP, ejecutando versiones de firmware anteriores a la versión 6.0.0.48;
- GS752TPv2, ejecutando versiones de firmware anteriores a la versión 6.0.0.48;
- GS808E, ejecutando versiones de firmware anteriores a la versión 1.7.0.7;
- GS908E, ejecutando versiones de firmware anteriores a la versión 1.7.0.3;
- GSS108E, ejecutando versiones de firmware anteriores a la versión 1.6.0.4;
- GSS108EPP, ejecutando versiones de firmware anteriores a la versión 1.0.0.15;
- SRK60, ejecutando versiones de firmware anteriores a la versión 2.3.5.106;
- SRR60, ejecutando versiones de firmware anteriores a la versión 2.3.5.106;
- SRS60, ejecutando versiones de firmware anteriores a la versión 2.3.5.106;
- WAC505, ejecutando versiones de firmware anteriores a la versión 5.6.8.3;
- WAC510, ejecutando versiones de firmware anteriores a la versión 5.6.8.3.

Descripción:

Netgear ha publicado 4 vulnerabilidades, dos de severidad crítica y dos 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:

- Las vulnerabilidades de severidad crítica podrían permitir a un atacante revelar información confidencial.
- Las vulnerabilidades de severidad alta podrían permitir a un atacante realizar un desbordamiento de búfer o de pila.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en Exim

Fecha de publicación: 09/09/2019

Importancia: Crítica

Recursos afectados:

Servidores Exim, versiones 4.92.1 y anteriores, que acepten conexiones TLS, tanto GnuTLS como OpenSSL.

Descripción:

Un fallo de seguridad crítico en Exim podría permitir la ejecución de código remoto con privilegios de root en servidores que aceptan conexiones TLS.

Solución:

Aplicar la actualización 4.92.2.

Detalle:

El envío de un SNI terminado en una secuencia *backslash-null* durante la negociación inicial de TLS, podría permitir a un atacante, local o remoto, ejecutar código con privilegios de administrador. Se ha asignado el identificador CVE-2019-15846 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en dispositivo N300 WNR2000v5 de Netgear

Fecha de publicación: 10/09/2019

Importancia: Alta

Recursos afectados:

Router Netgear N300 WNR2000v5, versión de *firmware* 1.0.0.70.

Descripción:

Dave McDaniel, de Cisco Talos, ha publicado dos vulnerabilidades de tipo denegación de servicio que afectan al router inalámbrico N300 WNR2000v5 de Netgear.

Solución:

Actualizar Netgear N300 WNR2000v5 a la versión 1.0.0.72.

Detalle:

- Existe una vulnerabilidad de denegación de servicio en la funcionalidad de gestión de sesiones del servidor HTTP en el producto Netgear N300 WNR2000v5. Una petición HTTP con una cadena de User-Agent vacía, enviada a una página que requiere autenticación, puede provocar la eliminación de un puntero nulo, lo que desembocaría en el bloqueo del servicio HTTP. Un atacante no autenticado puede enviar una petición HTTP especialmente diseñada para activar esta vulnerabilidad. Se ha reservado el identificador CVE-2019-5054 para esta vulnerabilidad.
- Existe una vulnerabilidad de denegación de servicio explotable en el Host Access Point Daemon (hostapd) del router inalámbrico Netgear N300 WNR2000v5. Una petición SOAP enviada en una secuencia inválida al servicio < *WFAWLANConfig:1#PutMessage* > puede causar una desreferencia de un puntero nulo, resultando en un fallo del servicio hostapd. Un atacante no autenticado puede enviar una solicitud SOAP especialmente diseñada para activar esta vulnerabilidad. Se ha reservado el identificador CVE-2019-5055 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Boletín de seguridad de Microsoft de septiembre de 2019

Fecha de publicación: 11/09/2019

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Internet Explorer;
- Microsoft Edge (basado en EdgeHTML);
- ChakraCore;
- Microsoft Office, Microsoft Office Services y Web Apps.;
- Adobe Flash Player;
- Microsoft Lync;
- Visual Studio;
- Microsoft Exchange Server;
- .NET Framework;
- Microsoft Yammer;
- .NET Core;
- ASP.NET;

- Team Foundation Server;
- Project Rome.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft correspondiente al mes de septiembre consta de 77 vulnerabilidades, 17 clasificadas como críticas y 60 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de información de la instalación de las mismas actualizaciones, se informa de los distintos métodos para llevarlas a cabo.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- elevación de privilegios;
- ejecución remota de código;
- divulgación de información;
- denegación de servicio;
- suplantación;
- omisión de característica de seguridad.

Etiquetas: Actualización, Adobe, Microsoft, Navegador, Vulnerabilidad, Windows

---

Actualización de seguridad de SAP de septiembre de 2019

Fecha de publicación: 11/09/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5;
- SAP Business One Client, versiones 9.2 y 9.3;
- SAP Business One, versión 9.3;
- SAP BusinessObjects Business Intelligence Platform (CMC), versiones 4.1, 4.2 y 4.3;
- SAP BusinessObjects Business Intelligence Platform, versiones 4.1 y 4.2;
- SAP Diagnostic Agent (LM-Service), versión 7.20;
- SAP HANA Extended Application Services, versiones anteriores a la 1.0.118;
- SAP HANA, versión 1.0, 2.0;
- SAP Kernel (RFC), versiones KRNL32NUC, KRNL32UC y KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 y KERNEL 7.21, 7.49, 7.53, 7.73, 7.76;
- SAP NetWeaver AS para Java (Web Container)-ENGINEAPI, versiones 7.10, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver Process Integration Runtime Workbench ? MESSAGING y SAP_XIA, versiones 7.31, 7.40 y 7.50;
- SAP Supplier Relationship Management (Master Data Management Catalog) (SRM_MDM_CAT), versiones 3.73, 7.31 y 7.32.

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 9 notas de seguridad y 4 actualizaciones, siendo 4 de ellas de severidad crítica, 1 alta, 7 medias y una baja.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de inyección de comandos en el sistema operativo;
- 2 vulnerabilidades de denegación de servicio;
- 2 vulnerabilidades de *Cross-Site Scripting* (XSS);
- 1 vulnerabilidad de escalada de privilegios;
- 1 vulnerabilidad de inyección de código;
- 5 vulnerabilidades de otro tipo.

Las notas de seguridad calificadas como críticas y alta se refieren a:

- Una vulnerabilidad de omisión de la comprobación de entrada de usuario. Un atacante podría inyectar código, como un contenido web dinámico, y provocar una ejecución no autorizada de comandos, revelar información sensible o generar una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-0355 para esta vulnerabilidad.
- Una actualización del boletín de abril de 2018.
- Una actualización del boletín de julio de 2019.
- Un atacante autenticado podría generar una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-0364 para esta vulnerabilidad.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 17/09/2019

Importancia: Alta

Recursos afectados:

Desde la versión 3.7 hasta 3.7.1, 3.6 hasta 3.6.5, 3.5 hasta 3.5.7 y versiones anteriores sin soporte.

Descripción:

Se han descubierto 6 vulnerabilidades en la plataforma Moodle, 2 de criticidad alta y 4 de criticidad baja.

Solución:

Actualizar a las versiones 3.7.2, 3.6.6 y 3.5.8.

Detalle:

- Una vulnerabilidad de criticidad alta podría permitir a un atacante inyección de código en algunas plantillas. Se ha reservado el identificador CVE-2019-14827 para esta vulnerabilidad.
- Una vulnerabilidad de criticidad alta podría dejar expuesto el *token* de acceso en usuarios que utilizasen un dispositivo móvil. Esto no afecta a usuarios que utilizasen la app como método de acceso o los sitios con un esquema de URL forzada configurado, con el servicio móvil desactivado. Se ha reservado el identificador CVE-2019-14830 para esta vulnerabilidad.
- Al resto de vulnerabilidades de severidad baja se les han reservado los identificadores CVE-2019-14828, CVE-2019-14829 y CVE-2019-14831.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 17/09/2019

Importancia: Alta

Recursos afectados:

- VMware vSphere ESXi, versiones 6.0, 6.5 y 6.7.
- VMware vCenter Server, versiones 6.0, 6.5 y 6.7.

Descripción:

Diversos investigadores han reportado 4 vulnerabilidades a VMware, dos de severidad media y dos de severidad alta, de tipo inyección de comandos y divulgación de información, que afectan a los productos vSphere ESXi y vCenter Server.

Solución:

- En VMware vSphere ESXi, aplicar los parches ESXi600-201909101-SG para la versión 6.0, ESXi650-201907101-SG para la versión 6.5 y ESXi670-201904101-SG para la versión 6.7.
- En VMware vCenter Server, aplicar los parches 6.0 U3j para la versión 6.0, 6.5 U3 / 6.5 U2b para la versión 6.5 y 6.7 U3 / 6.7 U1b para la versión 6.7.

Detalle:

- ESXi contiene una vulnerabilidad de inyección de comandos debido al uso de una versión vulnerable de *busybox* que no sanitiza los nombres de archivo, lo que puede resultar en la ejecución de comandos. Se ha asignado el identificador CVE-2017-16544 para esta vulnerabilidad.
- ESXi y vCenter son vulnerables a una divulgación de información en el lado del cliente, que surge de una expiración insuficiente de la sesión. Se ha reservado el identificador CVE-2019-5531 para esta vulnerabilidad.
- vCenter contiene una vulnerabilidad de divulgación de información debido al registro de credenciales en texto plano para máquinas virtuales desplegadas a través de OVF (*Open Virtualization Format*). Se ha reservado el identificador CVE-2019-5532 para esta vulnerabilidad.
- vCenter es vulnerable a una divulgación de información de inicio de sesión a través de las propiedades vAppCOnfig de la máquina virtual. Se ha reservado el identificador CVE-2019-5534 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos TIBCO

Fecha de publicación: 18/09/2019

Importancia: Crítica

Recursos afectados:

- TIBCO Enterprise Runtime para R - Server Edition, versiones 1.2.0 y anteriores.
- TIBCO Spotfire Analytics Platform para AWS Marketplace, versiones 10.4.0 y 10.5.0.

Descripción:

TIBCO ha detectado dos vulnerabilidades de severidad crítica. Un atacante remoto, no autenticado, podría omitir el acceso, revelar información confidencial o ejecutar código arbitrario.

Solución:

TIBCO ha publicado una serie de actualizaciones para solucionar las vulnerabilidades.

- TIBCO Enterprise Runtime para R - Server Edition, versiones 12.0 o anteriores, actualizar a la versión 12.1 o superior.
- TIBCO Spotfire Analytics Platform para AWS Marketplace, versiones 10.4.0 y 10.5.0, actualizar a la versión 10.5.1 o superior.

Detalle:

- Una vulnerabilidad podría permitir a un atacante remoto, no autenticado, omitir el acceso, revelar información confidencial o ejecutar código arbitrario en el sistema. Se ha reservado el identificador CVE-2019-11210 para esta vulnerabilidad.
- Una vulnerabilidad podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario, revelar información confidencial o tomar el control del sistema operativo. Se ha reservado el identificador CVE-2019-11211 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Exposición de información en BIG-IP ASM de F5

Fecha de publicación: 20/09/2019

Importancia: Crítica

Recursos afectados:

- VIPRION con BIG-IP ASM, versiones:
  - 15.0.0,
  - 14.0.0 y 14.1.0,
  - 13.1.0 - 13.1.1,
  - 12.1.0 - 12.1.4,
  - 11.6.1 - 11.6.4,
  - 11.5.2 - 11.5.9.

Descripción:

F5 ha detectado una vulnerabilidad de severidad crítica en sistemas VIPRION provistos de BIG-IP ASM.

Solución:

- Actualizar las siguientes versiones de BIG-IP ASM:
  - 15.0.1,
  - 14.1.2,
  - 14.0.1,
  - 13.1.3,
  - 12.1.5,
  - 11.6.5,
  - 11.5.10.

Detalle:

La vulnerabilidad se debe a un problema en sistemas VIPRION provistos de BIG-IP ASM, con interfaces de gestión en versiones anteriores de BIG-IP 14.1.0, o que dispongan del parámetro "Port Lockdown" configurado en "Allow All". Un atacante podría revelar información confidencial o modificar la configuración del sistema cuando no se utilizan los ajustes por defecto. Se ha reservado el identificador CVE-2019-6650 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 20/09/2019

Importancia: Alta

Recursos afectados:

- VMware vSphere ESXi, versiones 6.7, 6.5 y 6.0;
- VMware Workstation Pro / Player, versiones 15.x;
- VMware Fusion Pro / Fusion, versiones 11.x;
- VMware Remote Console (VMRC) para Windows y Linux, versiones 10.x;
- VMware Horizon Client para Windows, Linux y Mac, versiones 5.x y anteriores.

Descripción:

Diversos investigadores han reportado 2 vulnerabilidades a VMware, una de severidad alta y otra de severidad media, de uso después de liberación de memoria y denegación de servicio respectivamente, que afectan a varios productos de WMware.

Solución:

- En ESXi :
  - versión 6.7 aplicar el parche ESXi670-201904101-SG;
  - versión 6.5 aplicar el parche ESXi650-201903401-SG;
  - versión 6.0 aplicar el parche ESXi600-201909101-SG .
- Actualizar Workstation a la versión 15.5.0.
- Actualizar Fusion a la versión 11.5.0.
- Actualizar VMRC a la versión 10.0.5 o posterior.
- Actualizar Horizon Client a la versión 5.2.0.

Detalle:

- Los productos ESXi, Workstation, Fusion, VMRC y Horizon Client contienen una vulnerabilidad de uso después de liberación de memoria en el dispositivo de sonido virtual. Un atacante local, con acceso no administrativo en el equipo invitado, puede explotar esta vulnerabilidad para ejecutar código en el *host*. Se ha reservado el identificador CVE-2019-5527 para esta vulnerabilidad.
- Los productos Workstation y Fusion son vulnerables a un ataque de denegación de servicio en su red debido al tratamiento inadecuado de ciertos paquetes IPv6. Un atacante puede explotar esta vulnerabilidad enviando un paquete IPv6, especialmente diseñado, desde un equipo invitado en el NAT de VMware para impedir el acceso a la red a todos los equipos invitados que utilicen el modo NAT de VMware. Esta vulnerabilidad sólo puede ser explotada si el modo IPv6 para VMNAT está habilitado. Se ha reservado el identificador CVE-2019-5535 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades fuera de ciclo de Microsoft

Fecha de publicación: 24/09/2019

Importancia: Alta

Recursos afectados:

- Internet Explorer 11,
- Internet Explorer 10,
- Internet Explorer 9,
- Windows Defender,
- Microsoft Forefront Endpoint Protection 2010,
- Microsoft Security Essentials,
- Microsoft System Center 2012 Endpoint Protection,
- Microsoft System Center 2012 R2 Endpoint Protection,
- Microsoft System Center Endpoint Protection.

Descripción:

Microsoft ha corregido dos vulnerabilidades fuera de ciclo con criticidades altas. Un atacante remoto podría ejecutar código o generar una condición de denegación de servicio.

Solución:

Instalar las actualizaciones de seguridad correspondientes. En la página de información de la instalación de actualizaciones, se informa de los distintos métodos para llevarlas a cabo.

Detalle:

- Una vulnerabilidad se debe a una gestión inadecuada de ficheros en Microsoft Defender. Un atacante, con permisos de ejecución en el sistema, podría generar una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-1255 para esta vulnerabilidad.
- La otra vulnerabilidad se debe a la manera en la que el motor de *scripting* de Internet Explorer maneja los objetos en memoria. Un atacante remoto podría generar un sitio web malicioso con el fin de ejecutar código arbitrario u obtener los privilegios de usuario en el sistema. Se ha asignado el identificador CVE-2019-1367 para esta vulnerabilidad.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 25/09/2019

Importancia: Crítica

Recursos afectados:

- VMware Cloud Foundation.
- VMware Harbor Container Registry para PCF, versiones 18.x y 17.x.

Descripción:

Se ha reportado una vulnerabilidad de tipo escalada de privilegios, con severidad crítica, que afecta a múltiples productos de VMware.

Solución:

- En VMware Harbor Container Registry para PCF:
  - versiones 18.x, actualizar a la versión 1.8.3.
  - versiones 17.x, actualizar a la versión 1.7.6.
- VMware Cloud Foundation está afectado si el componente opcional *Harbor Registry* ha sido implementado, actualmente no actualización disponible.

Detalle:

La vulnerabilidad se encuentra en el método POST /api/users de la API de Harbor. Un atacante remoto podría realizar una escalada de privilegios. Se ha asignado el identificado CVE-2019-16097 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Vulnerabilidad en REST framework de múltiples productos de F5

Fecha de publicación: 25/09/2019

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,
  - 14.0.0 - 14.1.0,
  - 13.1.0 - 13.1.1,
  - 12.1.0 - 12.1.4,
  - 11.5.2 - 11.6.4.
- Enterprise Manager, versión 3.1.1.
- BIG-IQ Centralized Management, versiones:
  - 7.0.0,
  - 6.0.0 - 6.1.0,
  - 5.2.0 - 5.4.0.
- F5 iWorkflow, versión 2.3.0.

Descripción:

El equipo Enter of the Tarantula, perteneciente a VINCSS, una empresa subsidiaria del grupo Vingroup, en coordinación con F5, ha detectado una vulnerabilidad de criticidad alta en el componente REST framework. Un atacante podría comprometer el sistema.

Solución:

Actualizar a las siguientes versiones:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 15.0.1,
  - 14.1.2,
  - 14.0.1,
  - 13.1.3,
  - 12.1.5,
  - 11.6.5.

En este momento no hay actualizaciones disponibles para el resto de productos afectados, como medidas de mitigación. Desde F5 recomiendan el uso de redes seguras y permitir el acceso únicamente a usuarios de confianza en los sistemas afectados.

Detalle:

La vulnerabilidad se debe a respuestas HTTP inconsistentes en el inicio de sesión, cuando se procesan peticiones modificadas. Un atacante podría enviar peticiones maliciosas para explotar vulnerabilidades en el sistema. Se ha reservado el identificador CVE-2019-6651 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de ejecución remota en e2fsprogs

Fecha de publicación: 25/09/2019

Importancia: Alta

Recursos afectados:

E2fsprogs, versiones anteriores a 1.45.4.

Descripción:

La investigadora Lilith, de Cisco Talos, ha descubierto una vulnerabilidad de tipo ejecución de código, con severidad alta, en e2fsprogs, un paquete de utilidades para el mantenimiento de sistemas de ficheros ext2, ext3 y ext4.

Solución:

Actualizar e2fsprogs a la versión 1.45.4.

Detalle:

Un sistema de particiones ext4, específicamente generado, podría causar una escritura fuera de límites en la memoria dinámica (*heap*) en la funcionalidad *quota* utilizada por *e2fsck*. Un atacante podría ejecutar código arbitrario en el sistema. Se ha asignado el identificador CVE-2019-5094 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.12

Fecha de publicación: 25/09/2019

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones desde la 3.0.0 hasta la 3.9.11.

Descripción:

Joomla! ha publicado una nueva versión que soluciona una vulnerabilidad, de criticidad baja, en su núcleo de tipo *cross-site scripting* (XSS).

Solución:

Actualizar a la versión 3.9.12.

Detalle:

La vulnerabilidad en el parámetro *logo* en las plantillas por defecto permitía un escapado inadecuado de código, pudiendo generar un XSS. Se ha asignado el identificador CVE-2019-16725 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 26/09/2019

Importancia: Alta

Recursos afectados:

- Productos Cisco que ejecuten una versión vulnerable de Cisco IOS o IOS XE y que estén configurados para responder a las solicitudes del protocolo Ident.
- Switches Cisco Catalyst 3850 y 9300 que ejecuten una versión vulnerable del software Cisco IOS XE.
- Software Cisco IOS XE si el dispositivo tiene una interfaz con UTD con una dirección IPv6 habilitada y si el dispositivo está configurado con la función Snort IPS de Cisco UTD, la función de filtrado basada en URL de Cisco UTD, o ambas.
- Dispositivos que ejecutan una versión vulnerable del software Cisco IOS XE y que están configurados con NAT, NAT64 o ZBFW con la inspección FTP habilitada.
- Los siguientes productos de Cisco si están configurados con el entorno de aplicación Cisco IOx y ejecutando una versión de software anterior a la primera versión solucionada:
  - Cisco 510 WPAN Industrial Router: Industrial Routers Operating System Software,
  - Cisco CGR 1000 Compute Module: CGR 1000 IOx Compute Platform Firmware,
  - Cisco IC3000 Industrial Compute Gateway: Industrial Compute Gateway Software,
  - Cisco Industrial Ethernet 4000 Series Switches: Cisco IOS Software.
- Dispositivos Cisco que ejecutan una versión vulnerable de Cisco IOS XE Software.
- Routers de la serie ASR 900 de Cisco con la versión 16.9 del software Cisco IOS XE y que están configurados como un servidor Raw Socket TCP. Opción no habilitada por defecto.
- Routers Cisco con una versión vulnerable de Cisco IOS o IOS XE y con cualquiera de las siguientes funciones habilitadas:
  - Cisco Unified Border Element (CUBE),
  - Cisco Unified Communications Manager Express (CME),
  - Cisco IOS Gateways with Session Initiation Protocol (SIP),
  - Cisco TDM Gateways,
  - Cisco Unified Survivable Remote Site Telephony (SRST),
  - Cisco Business Edition 4000 (BE4K).
- Dispositivos Cisco con una versión vulnerable del software IOS XE y con la función de HTTP Server activada.
- Routers Cisco 800 Series Industrial Integrated Services Routers y Cisco 1000 Series Connected Grid Routers (CGR 1000) con una versión vulnerable del software Cisco IOS con Guest OS instalado.
- Los siguientes dispositivos Cisco con una versión vulnerable del software Cisco IOS:
  - Cisco Catalyst 4500 Supervisor Engine 6-E,
  - Cisco Catalyst 4500 Supervisor Engine 6L-E,
  - Cisco Catalyst 4900M Switch,
  - Cisco Catalyst 4948E Ethernet Switch,
  - Cisco Catalyst 4948E-F Ethernet Switch.
- Los siguientes dispositivos Cisco con una versión vulnerable del software Cisco IOS XE que está configurado para funcionar con NAT:
  - Cisco 1100, 4200, and 4300 Integrated Services Routers (ISRs),
  - Cisco Cloud Services Router (CSR) 1000V Series,
  - Cisco Enterprise Network Compute System (ENCS),
  - Cisco Integrated Services Virtual Router (ISRv).

Descripción:

Cisco ha publicado 12 vulnerabilidades de severidad alta que afectan a sus productos.

Solución:

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

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades descritas en este aviso, podría llegar a realizar alguna de las siguientes acciones:

- recargar un dispositivo afectado;
- instalar y arrancar una imagen de software malicioso o ejecutar binarios no firmados;
- denegar el servicio;
- ejecutar comandos con privilegios de administrador u obtener acceso no autorizado al sistema operativo invitado (SO invitado).

Para estas vulnerabilidades, se han asignado los siguientes identificadores: CVE-2019-12647, CVE-2019-12649, CVE-2019-12657, CVE-2019-12655, CVE-2019-12656, CVE-2019-12658, CVE-2019-12653, CVE-2019-12654, CVE-2019-12650, CVE-2019-12651, CVE-2019-12648, CVE-2019-12652 y CVE-2019-12646.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Ejecución remota de código en Exim

Fecha de publicación: 30/09/2019

Importancia: Crítica

Recursos afectados:

Todas las versiones desde la 4.92 hasta la 4.92.2 (ambas inclusive).

Descripción:

Se ha publicado una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (heap) en string_vformat (string.c) que podría permitir a un atacante la ejecución remota de código.

Solución:

Actualizar a la versión 4.92.3.

Detalle:

Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (heap) en string_vformat (string.c) podría permitir a un atacante la ejecución remota de código o la denegación del servicio, utilizando una cadena EHLO extraordinariamente larga para bloquear el proceso Exim que esté recibiendo el mensaje. Se ha asignado el identificador CVE-2019-16928 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad