Boletín de febrero de 2019

Avisos Técnicos

Vulnerabilidad de inyección de código en IBM Security Identity Manager

Fecha de publicación: 01/02/2019

Importancia: Alta

Recursos afectados:

- IBM Security Identity Manager, versiones desde la 6.0.0 hasta la 6.0.0.20
- IBM Security Identity Manager VA, versiones desde la 7.0.0 hasta la 7.0.1.10

Descripción:

IBM ha publicado una vulnerabilidad en IBM Security Identity Manager (ISIM) que permitiría a un atacante poner en riesgo las cuentas de los usuarios mediante una inyección de código limitada.

Solución:

- IBM Security Identity Manager aplicar el parche 6.0.0-ISS-SIM-FP0021.
- IBM Security Identity Manager VA aplicar el parche 7.0.1-ISS-SIM-FP0011.

Detalle:

- Una vulnerabilidad en IBM Security Identity Manager posibilitaría a un atacante crear rutas de flujo de control inesperadas a través de la aplicación, que le permitiría evitar las comprobaciones de seguridad e inyectar código de una forma limitada. Se ha reservado el identificador CVE-2019-4038 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad en tokens de acceso en IBM API Connect V2018

Fecha de publicación: 04/02/2019

Importancia: Crítica

Recursos afectados:

- IBM API Connect, versiones desde 2018.1 hasta 2018.4.1.1

Descripción:

Se ha detectado una vulnerabilidad de severidad crítica en IBM API Connect, donde podrían verse comprometidos los *tokens* de acceso.

Solución:

- IBM ha publicado una actualización para mitigar la vulnerabilidad en la versión 2018.4.1.2

Detalle:

- Esta vulnerabilidad de severidad crítica permitiría a un atacante, en ciertas URLs, escribir los *tokens* de autorización en un archivo de *log*. Se ha reservado el identificador CVE-2019-4008 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 05/02/2019

Importancia: Alta

Recursos afectados:

- HPE Integrated Lights-Out 5 (iLO 5) para HPE Gen10 Servers versiones anteriores a v1.40.
- HPE Service Pack para ProLiant versiones anteriores a 2018.09.0 (27 Sep 2018).

Descripción:

Se han detectado varias vulnerabilidades en productos de HPE que podrían permitir una ejecución remota de código (XSS) o eludir la restricción de acceso local.

Solución:

- Para HPE Integrated Lights-Out 5 (iLO 5) actualizar el firmware a la versión 1.40 o posterior.
- Para HPE Service Pack para ProLiant (SPP) actualizar a la versión 2018.09.0(27 Sep 2018) o posterior.

Detalle:

- Un atacante remoto podría explotar la vulnerabilidad de iLO de HP que permitiría la ejecución de código arbitrario a través del interfaz web de usuario. Se ha reservado el identificador CVE-2018-7117 para esta vulnerabilidad de severidad alta.
- Un atacante con acceso local podría omitir las restricciones de acceso en HPE Service Pack ProLiant. Se ha reservado el identificador CVE-2018-7118 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Intelligent Management Center de HPE

Fecha de publicación: 06/02/2019

Importancia: Crítica

Recursos afectados:

- Intelligent Management Center

Descripción:

Matthias Kaiser y Steven Seeley, de Incite Team, han publicado un total de 12 vulnerabilidades, siendo una de ellas de severidad media, 9 altas y 2 críticas. Todas ellas podrían permitir la ejecución remota de código arbitrario.

Solución:

- Aún no existe actualización que corriga estas vulnerabilidades. Como medida de mitigación, se recomienda permitir únicamente a máquinas de confianza la interacción con el servicio.

Detalle:

Las vulnerabilidades de severidad crítica son:

- El filtrado inadecuado de las URLs presente en el servlet *UrlAccessController* podría permitir a un atacante sin autentificación acceder a recursos protegidos del usuario mediante la escalada de privilegios.
- La gestión incorrecta del parámetro benName proporcionado por el endpoint *iccSelectCommand.xhtml* provoca una validación incorrecta de la cadena suministrada por el usuario, antes de usarla para renderizar una página, lo que podría permitir a un atacante remoto ejecutar código arbitrario en las instalaciones vulnerables del producto afectado.

Etiquetas: 0day, HP, Vulnerabilidad

Vulnerabilidad en sistemas inalámbricos Avastar de Marvell

Fecha de publicación: 06/02/2019

Importancia: Alta

Recursos afectados:

Sistema en chip (*System on Chip*, SoC) inalámbrico Marvell Avastar, versiones:

- 88W8787
- 88W8797
- 88W8801
- 88W8897

Descripción:

Algunos modelos de sistemas en chip (*Systems on Chip*, SoC) inalámbricos Marvell Avastar contienen múltiples vulnerabilidades, incluyendo un desbordamiento de espacio de memoria en bloques durante el escaneo de la red Wi-Fi.

Solución:

- Marvell emitió un informe y aconseja a los clientes ponerse en contacto con su representante de Marvell para obtener asistencia adicional. Microsoft publicó una actualización para dispositivos Surface Pro 3 en Windows 10 Creators Update, versión 1703 o superior.

Detalle:

- Durante los escaneos de red Wi-Fi, se puede desencadenar una condición de desbordamiento, sobrescribiendo ciertas estructuras en bloque del *pool* de datos. Un atacante no autenticado dentro del alcance de la radio Wi-Fi utilizaría una serie de *frames* Wi-Fi especialmente diseñados para ejecutar código arbitrario en un sistema con un SoC de Marvell vulnerable. Dependiendo de la implementación, el SoC comprometido puede utilizarse para interceptar el tráfico de red o lograr la ejecución de código en el sistema *host*. Se ha asignado el identificador CVE-2019-6496 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Microsoft, Vulnerabilidad

---

Vulnerabilidad en MaaS360 de IBM para iOS

Fecha de publicación: 08/02/2019

Importancia: Alta

Recursos afectados:

- Aplicación MaaS360 para iOS, versión 3.30 y anteriores.

Descripción:

Una vulnerabilidad de severidad alta podría permitir a un atacante acceder a información sensible.

Solución:

- Actualizar la aplicación a la versión 3.40 o superior.

Detalle:

- La aplicación contiene credenciales por defecto embebidas en el código, un atacante podría emplear dichas credenciales para obtener acceso y revelar información sensible. Se ha reservado el identificador CVE-2018-1960 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en Nginx Unit

Fecha de publicación: 08/02/2019

Importancia: Alta

Recursos afectados:

- Nginx Unit desde la versión 0.3 hasta la 1.7

Descripción:

Se ha publicado una vulnerabilidad en Nginx unit que podría permitir a un atacante provocar una denegación de servicio u otro comportamiento no especificado.

Solución:

- El problema se ha solucionado en Unit 1.7.1

Detalle:

- La vulnerabilidad podría permitir a un atacante causar un desbordamiento del búfer de memoria en el proceso de enrutado con una petición especialmente diseñada. Esto puede resultar en una denegación de servicio (fallo del proceso del router) u otro comportamiento no especificado. Se ha reservado el identificador CVE-2019-7401 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Vulnerabilidad XXE en InfoSphere Information Server de IBM

Fecha de publicación: 12/02/2019

Importancia: Alta

Recursos afectados:

- IBM InfoSphere Information Server: versiones 9.1, 11.3, 11.5 y 11.7
- IBM InfoSphere Information Server on Cloud: versiones 11.5 y 11.7

Descripción:

Se ha detectado una vulnerabilidad de criticidad alta que podría permitir a un atacante obtener información sensible o consumir recursos de memoria.

Solución:

- Desde IBM recomiendan evitar utilizar la opción de importar XML. En su lugar, emplear el botón *ADD* para agregar información.
- En caso de que se necesite importar un XML, se recomienda comprobar manualmente el archivo XML antes de importarlo. Si hay una sección *DTD/DOCTYPE*, verificar el contenido para detectar cualquier posible código sospechoso.

Detalle:

- IBM InfoSphere Information Server es vulnerable a un ataque del tipo XXE (XML *External Entity Injection*) cuando se procesan datos XML. Un atacante remoto podría explotar esta vulnerabilidad y exponer información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2018-1727 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Vulnerabilidad de credenciales por defecto en Network Assurance Engine de Cisco

Fecha de publicación: 13/02/2019

Importancia: Alta

Recursos afectados:

- Cisco Network Assurance Engine versión 3.0 (1)

Descripción:

Cisco ha publicado una vulnerabilidad en la interfaz web de administración de Cisco Network Assurance Engine (NAE), que permitiría a un atacante local no autenticado obtener acceso no autorizado o provocar una condición de denegación de servicio (DoS) en el servidor.

Solución:

- Actualizar a la versión 3.0 (1a) y cambiar la contraseña de administrador predeterminada desde la CLI mediante el comando *passwd*.

Detalle:

- La vulnerabilidad se debe a un fallo en el sistema de gestión de contraseñas de NAE, por el que un atacante podría autenticarse con la contraseña de administrador predeterminada a través de la CLI de un servidor afectado. La explotación exitosa podría permitir al atacante ver información sensible o desactivar el servidor, causando una condición DoS. Se ha asignado el identificador CVE-2019-1688 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 13/02/2019

Importancia: Crítica

Recursos afectados:

- Componente de servidor de software Intel Unite® Solution, versiones desde 3.2 hasta 3.3
- Intel(R) Data Center Manager SDK, versiones anteriores a 5.0.2
- Intel® USB 3.0 eXtensible Host Controller Driver para Microsoft Windows® 7, versiones anteriores a 5.0.4.43v2
- OpenVINO™ 2018 para Linux, versiones anteriores a R4
- Intel® PROSet Wireless Driver, versiones anteriores (e incluyendo) 20.50

Descripción:

Intel ha publicado 5 avisos en su centro de seguridad de productos que contienen 15 vulnerabilidades, repartidas en una de severidad crítica, 3 de severidad alta, 7 de severidad media y 4 de severidad baja.

Solución:

- Actualizar a la última versión del producto afectado disponible en su centro de descargas.

Detalle:

Las vulnerabilidades de severidad crítica y alta son las siguientes:

- Una omisión de autenticación en el producto Intel Unite(R) permitiría a un usuario no autenticado habilitar la escalada de privilegios al portal administrativo a través del acceso a la red. Se ha reservado el identificador CVE-2019-0101 para esta vulnerabilidad.
- Una autenticación de sesión insuficiente en el servidor web para el SDK de Intel(R) Data Center Manager permitiría a un usuario no autenticado habilitar la escalada de privilegios a través del acceso a la red. Se ha reservado el identificador CVE-2019-0102 para esta vulnerabilidad.
- Un insuficiente aviso al usuario en la rutina de instalación del SDK de Intel(R) Data Center Manager permitiría a un usuario privilegiado habilitar la escalada de privilegios a través del acceso local. Se ha reservado el identificador CVE-2019-0107 para esta vulnerabilidad.

- Una gestión insuficiente de las claves del SDK de Intel(R) Data Center Manager permitiría que un usuario autenticado habilite la divulgación de información a través del acceso local. Se ha reservado el identificador CVE-2019-0110 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han reservado los identificadores CVE-2019-0103, CVE-2019-0104, CVE-2019-0105, CVE-2019-0106, CVE-2019-0108, CVE-2019-0109, CVE-2019-0111, CVE-2019-0112, CVE-2018-3700, CVE-2019-0127 y CVE-2018-12159.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de febrero de 2019

Fecha de publicación: 13/02/2019

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player
- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office, Microsoft Office Services y Web Apps
- ChakraCore
- .NET Framework
- Microsoft Exchange Server
- Microsoft Visual Studio
- Azure IoT SDK
- Microsoft Dynamics
- Team Foundation Server
- Visual Studio Code

Descripción:

La publicación de actualizaciones de seguridad de Microsoft este mes consta de 73 vulnerabilidades, 20 clasificadas como críticas y 53 como importantes, siendo el resto de las publicadas de severidad media o baja.

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:

El tipo de vulnerabilidades publicadas se corresponde con las siguientes:

- Ejecución remota de código.
- Revelación de información.
- Escalado de privilegios.
- Suplantación.
- Evasión de seguridad.

Etiquetas: Actualización, Microsoft, Navegador, Sistema Operativo, Vulnerabilidad

---

Actualización de seguridad de Joomla! 3.9.3

Fecha de publicación: 13/02/2019

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones desde la 1.0.0 hasta la 3.9.2

Descripción:

Joomla! ha publicado una nueva versión que soluciona seis vulnerabilidades en el núcleo, todas ellas de criticidad baja.

Solución:

- Actualizar a la versión 3.9.3

Detalle:

- El filtrado inadecuado de los campos URL en varios componentes del *core* podrían permitir ataques XSS. Se ha asignado el identificador CVE-2019-7743 para esta vulnerabilidad.
- Una serie de configuraciones específicas de servidor web en combinación con tipos de archivos específicos y "mime-type sniffing" en el lado del navegador, podría permitir ataques XSS. Se ha asignado el identificador CVE-2019-7742 para esta vulnerabilidad.
- El filtro de texto "No Filtering" sobreescribe la configuración secundaria en "Global configuration". Este es un comportamiento intencionado que podía resultar inesperado para el usuario. Se ha asignado el identificador CVE-2019-7739 poara esta vulnerabilidad.
- Las comprobaciones inadecuadas en los ajustes del "helpurl" de "Global configuration" podrían permitir un XSS persistente. Se ha asignado el identificador CVE-2019-7741 para esta vulnerabilidad.
- Un manejo inadecuado de los parámetros en el código JS podría permitir ataques de XSS. Se ha asignado el identificador CVE-2019-7740 para esta vulnerabilidad.
- El envoltorio de flujos phar:// se puede utilizar para llevar a cabo ataques de inyección de objeción. Se ha asignado el identificador CVE-2019-7743 para esta vulnerabilidad.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

Contraseña insegura en Rational ClearCase GIT connector de IBM

Fecha de publicación: 14/02/2019

Importancia: Alta

Recursos afectados:

- IBM Rational ClearCase GIT connector versión 1.0.0.0

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta debida a una mala protección de la contraseña de la base de datos de documentos.

Solución:

- Actualizar a la versión IBM Rational ClearCase GIT connector 1.0.0.1

Detalle:

- La vulnerabilidad detectada se debe a una insuficiente protección de la contraseña de la base de datos de documentos, un atacante podría obtener la contraseña para acceder a ella. Se ha reservado el identificador CVE-2019-4059 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Actualización de seguridad de SAP de febrero de 2019

Fecha de publicación: 14/02/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5
- SAP Landscape Management, versiones VCM 3.0
- ABAP Platform (SLD Registration), versiones KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49; KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73; KERNEL desde 7.21 hasta 7.22, 7.45, 7.49, 7.53, 7.73, 7.75
- SAP Disclosure Management, versión 10.01
- Solution Tools Plug-In (ST-PI); versiones 2008_1_700, 2008_1_710, 740
- ABAP Platform, versiones Krnl64nuc 7.74, krnl64UC 7.73, 7.74, Kernel 7.73, 7.74, 7.75
- SAP_BASIS, versiones desde 7.00 hasta 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51
- SAP HANA Extended Application Services, modelo avanzado (XS advanced), versión 1.0
- SAP Disclosure Management, versión 10.01 Stack 1301
- SAP BusinessObjects Business Intelligence Platform Servers (Enterprise), versiones 4.2, 4.3
- SAP Manufacturing Integration and Intelligence, versiones 15.0, 15.1 y 15.2
- SAP BusinessObjects Business Intelligence Platform, versiones 4.2, 4.3
- SAP Business One Mobile Android App, versión 1.2.12
- ABAP Platform (SAP Basis), versiones desde 7.0 hasta 7.02, desde 7.10 hasta 7.11, 7.30, 7.31, 7.40, desde 7.50 hasta 7.53, desde 7.74 hasta 7.75
- SAP Enterprise Architecture Designer para SAP HANA, versión 1.0
- SAP WebIntelligence BILaunchPad (Enterprise), versiones 4.10, 4.20

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, siendo 2 de ellas de severidad crítica, 4 altas y 10 medias.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de falta de comprobación de autorización.
- 3 vulnerabilidades de XSS (*Cross-Site Scripting*).
- 3 vulnerabilidades de revelación de información.
- 1 vulnerabilidad de falta de autenticación.
- 2 vulnerabilidades de falta de validación de XML.
- 5 vulnerabilidades de otro tipo.

Las notas de seguridad calificadas como críticas se refieren a:

- Actualizaciones de seguridad para el control del navegador Chromium suministradas con SAP Business Client.
- Comprobación de falta de autenticación en el modelo avanzado de SAP HANA Extended Application Services que permitiría a un atacante no solo leer, modificar o eliminar información sensible, sino también obtener funcionalidades con privilegios elevados. Se ha reservado el identificador CVE-2019-0261 para esta vulnerabilidad.

Las notas de seguridad calificadas como altas se refieren a:

- Vulnerabilidad de tipo XXE (*XML External Entity)* en SLD Registration de ABAP Platform. Se ha reservado el identificador CVE-2019-0265 para esta vulnerabilidad.
- Falta de autorización en SAP Disclosure Management. Se ha reservado el identificador CVE-2019-0258 para esta vulnerabilidad.
- Divulgación de información relacionada con el sistema de archivos del servidor de bases de datos.
- ABAP Platform proporciona acceso a Easy Access Menu. Se ha reservado el identificador CVE-2019-0255 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han reservado los identificadores CVE-2019-0266, CVE-2019-0254, CVE-2019-0259, CVE-2019-0267, CVE-2019-0251, CVE-2019-0256, CVE-2019-0257 y CVE-2019-0262.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad en el container runc de VMware

Fecha de publicación: 18/02/2019

Importancia: Alta

Recursos afectados:

- VMware Integrated OpenStack con Kubernetes (VIO-K), versiones 5.x
- VMware PKS (PKS), versiones 1.3.x y 1.2.x
- VMware vCloud Director Container Service Extension (CSE), versiones 1.x
- vSphere Integrated Containers (VIC), versiones 1.x

Descripción:

Se ha publicado una actualización de productos VMware que resuelve una vulnerabilidad en la gestión del descriptor de ficheros en tiempo de ejecución del contenedor *runc*.

Solución:

Actualizar el producto a las siguientes versiones:

- VMware PKS (PKS) versiones 1.3.x y 1.2.x, actualizar a la versión 1.3.2 y 1.2.9 respectivamente.
- VMware vCloud Director Container Service Extension (CSE) versiones 1.x, actualizar a la versión 1.2.7

Detalle:

- La actualización de VMware resuelve una vulnerabilidad en la gestión de la descripción de ficheros en tiempo de ejecución del contenedor *runc*. La explotación de esta vulnerabilidad podría permitir que un contenedor malicioso sobreescribiera los contenidos del binario *runc* del *host* y ejecutara código arbitrario. El atacante debe tener permisos de ejecución o permisos para desplegar contenedores, o engañar a un usuario para conseguirlos. Se ha asignado el identificador CVE-2019-5736 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 21/02/2019

Importancia: Alta

Recursos afectados:

- Cisco HyperFlex Software, versiones anteriores a 3.5 (2a).
- Cisco IOS XR Software, versiones anteriores a 6.5.2 para dispositivos Cisco Network Convergence System 1000 Series con el servicio TFTP activado.
- Cisco PCA Software, versiones anteriores a 12.1 SP2.
- Cisco Prime Infrastructure (PI) Software, versiones desde 2.2 hasta 3.4.0, donde PI server esté integrado con ISE (desactivado por defecto).

Descripción:

Se han publicado 5 vulnerabilidades de severidad alta en productos Cisco que podrían permitir a un atacante escalar privilegios, ejecutar código con permisos de *root*, divulgar información, acceder al sistema o ver e interceptar comunicaciones.

Solución:

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

Detalle:

- Los controles de autenticación insuficientes podrían permitir a un atacante conectarse al servicio *hxterm* como un usuario local sin privilegios y obtener acceso de *root* a todos los nodos del clúster HyperFlex. Se ha reservado el identificador CVE-2019-1664 para esta vulnerabilidad.
- La validación de entrada insuficiente podría permitir a un atacante conectarse al administrador de servicios de clúster Cisco HyperFlex y ejecutar comandos como usuario *root* en el *host* afectado. Se ha asignado el identificador CVE-2018-15380 para esta vulnerabilidad.
- La validación incorrecta de las entradas suministradas por el usuario en las solicitudes FTP podría permitir a un atacante recuperar archivos arbitrarios del dispositivo afectado, lo que daría como resultado la revelación de información sensible. Se ha reservado el identificador CVE-2019-1681 para esta vulnerabilidad.
- El control de autenticación insuficiente en el servicio Quality of Voice Reporting (QOVR) del software Cisco Prime Collaboration Assurance (PCA) podría permitir a un atacante remoto no autenticado acceder al sistema con un nombre de usuario válido. Se ha reservado el identificador CVE-2019-1662 para esta vulnerabilidad.
- La validación incorrecta del certificado SSL del servidor al establecer el túnel SSL con ISE que podría permitir a un atacante utilizar un certificado SSL especialmente diseñado para ver e interceptar las comunicaciones entre el ISE y el PI. Se ha reservado el identificador CVE-2019-1659 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en el core de Drupal

Fecha de publicación: 21/02/2019

Importancia: Crítica

Recursos afectados:

- Módulos contribuidos de Drupal 7.x
- Drupal 8.x

Descripción:

El equipo de seguridad de Drupal ha detectado una vulnerabilidad de severidad crítica en el *core*, que podría permitir a un atacante remoto comprometer un sitio web basado en Drupal.

Solución:

Drupal recomienda actualizar en función de la versión que se disponga.

- Versión de Drupal 8.6.x, actualizar a Drupal 8.6.10.
- Versión de Drupal 8.5.x o anteriores, actualizar a Drupal 8.5.11.
- Asegurarse de instalar las actualizaciones de seguridad disponibles para los proyectos contribuidos después de actualizar el núcleo de Drupal.
- No se requiere ninguna actualización del núcleo para Drupal 7, pero varios módulos aportados por Drupal 7 requieren actualizaciones.

Versiones de Drupal 8 anteriores a 8.5.x son *end-of-life* y no recibirán cobertura de seguridad.

Detalle:

- Esta vulnerabilidad permite que algunos tipos de campo no validen correctamente los datos de fuentes que no son formularios, lo que puede llevar a la ejecución arbitraria de código PHP en algunos casos. Se ha reservado el identificador CVE-2019-6340 para esta vulnerabilidad.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

Vulnerabilidad de fuga de memoria en ISC BIND

Fecha de publicación: 22/02/2019

Importancia: Alta

Recursos afectados:

- BIND, versiones desde 9.10.7 hasta 9.10.8-P1, desde 9.11.3 hasta 9.11.5-P1 y desde 9.12.0 hasta 9.12.3-P1
- BIND 9 Supported Preview Edition, versiones desde 9.10.7-S1 hasta 9.11.5-S3
- Rama de desarrollo 9.13 de BIND, versiones desde 9.13.0 hasta 9.13.6

Descripción:

El investigador Toshifumi Sakaguchi ha descubierto una vulnerabilidad en ISC BIND de severidad alta que podría provocar una fuga de memoria en el sistema afectado.

Solución:

- Actualizar a una versión de BIND que contenga una solución para esta vulnerabilidad:
  - BIND 9.11.5-P4
  - BIND 9.12.3-P4
- BIND Supported Preview Edition es una rama de BIND que ofrece una vista previa de características especiales a los clientes elegibles de soporte ISC:
  - BIND 9.11.5-S5

Detalle:

- La vulnerabilidad puede producir un fallo en la memoria libre cuando se procesan mensajes que tienen una combinación específica de opciones EDNS. Al explotar este fallo, un atacante puede hacer que el uso de la memoria crezca sin límites hasta que se agote toda la memoria disponible para el proceso. Usualmente, un proceso del servidor está limitado en cuanto a la cantidad de memoria que puede usar, pero si dicho proceso no está controlado por el sistema operativo, toda la memoria libre en el servidor podría agotarse. Se ha reservado el identificador CVE-2018-5744 para esta vulnerabilidad.

Etiquetas: Actualización, DNS, Vulnerabilidad

Vulnerabilidad en BIG-IP de F5

Fecha de publicación: 26/02/2019

Importancia: Alta

Recursos afectados:

- BIG-IP, versión 14.1.0

Descripción:

Una vulnerabilidad de criticidad alta en BIG-IP podría reiniciar el TMM (*Traffic Management Microkernel*) y temporalmente fallar al procesar el tráfico.

Solución:

- Actualizar BIG-IP a la versión 14.1.0.2

Detalle:

- La vulnerabilidad podría reiniciar el TMM y generar un archivo *core* al validar certificados SSL en perfiles SSL de cliente o servidor. Se ha reservado el identificador CVE-2019-6592 para esta vulnerabilidad.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 28/02/2019

Importancia: Crítica

Recursos afectados:

- Cisco RV110W Wireless-N VPN Firewall, versiones anteriores a 1.2.2.1
- Cisco RV130W Wireless-N Multifunction VPN Router, versiones anteriores a 1.0.3.45
- Cisco RV215W Wireless-N VPN Router, versiones anteriores a 1.3.1.1
- Cisco Webex Meetings Desktop App, versiones anteriores a 33.6.6
- Cisco Webex Productivity Tools, versiones 32.6.0 y posteriores, pero anteriores a 33.0.7

Descripción:

Se ha publicado una vulnerabilidad de severidad crítica que permite a un atacante remoto, sin autenticar, la ejecución de código arbitrario en el dispositivo afectado, y otra vulnerabilidad de severidad alta que permite a un atacante local autenticado ejecutar comandos arbitrarios como usuario con privilegios.

Solución:

Cisco ha corregido estas vulnerabilidades en las siguientes versiones de los productos afectados, que pueden descargarse desde el panel de descarga de software:

- Cisco RV110W Wireless-N VPN Firewall, versión 1.2.2.1
- Cisco RV130W Wireless-N Multifunction VPN Router, versión 1.0.3.45
- Cisco RV215W Wireless-N VPN Router, versión 1.3.1.1
- Cisco Webex Meetings Desktop App, versiones 33.6.6 y 33.9.1
- Cisco Webex Productivity Tools, versión 33.0.7

Detalle:

- La vulnerabilidad crítica se origina debido a la validación incorrecta de los datos suministrados por el usuario en la interfaz de gestión basada en web. Un atacante podría explotar esta vulnerabilidad enviando solicitudes HTTP maliciosas a un dispositivo específico, lo que daría la posibilidad al atacante de ejecutar código arbitrario en el sistema operativo subyacente del dispositivo afectado como usuario con altos privilegios. Se ha asignado el identificador CVE-2019-1663 para esta vulnerabilidad.
- La vulnerabilidad alta se debe a la insuficiente validación de los parámetros suministrados por el usuario. Un atacante podría explotar esta vulnerabilidad invocando el comando *update service* con un argumento especialmente diseñado, lo que permitiría al atacante ejecutar comandos arbitrarios con privilegios de usuario de *SYSTEM*. Se ha reservado el identificador CVE-2019-1674 para esta vulnerabilidad

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad 0-byte record padding oracle en OpenSSL

Fecha de publicación: 28/02/2019

Importancia: Media

Recursos afectados:

- OpenSSL 1.0.2

Descripción:

OpenSSL ha publicado una vulnerabilidad de tipo 0-byte record padding oracle que podría permitir a un atacante remoto descifrar datos y obtener información confidencial.

Solución:

- Actualizar a las versiones 1.0.2r o 1.1.1

Actualmente solo reciben actualizaciones de seguridad OpenSSL las versiones 1.0.2 y 1.1.0. Para la versión 1.0.2, el soporte finalizará el 31 de diciembre de 2019 y para la versión 1.1.0, el 11 septiembre de 2019. Los usuarios de estas versiones deben actualizar a OpenSSL 1.1.1

Detalle:

- Si una aplicación encuentra un error fatal de protocolo y luego llama dos veces a la función *SSL_shutdown(),* una para enviar *close_notify* y otra para recibirlo, OpenSSL podría responder de forma diferente a la aplicación que llama, dependiendo de si recibe un registro de 0 bytes con un *padding* inválido o de si recibe un registro de 0 bytes con una MAC inválida. Si la aplicación se comporta de forma diferente a lo esperado por el *remote peer*, se podrían descifrar datos y obtener información confidencial mediante un ataque de *padding oracle*. Se ha asignado el identificador CVE-2019-1559 para esta vulnerabilidad.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad