Boletín de junio de 2019

Avisos Técnicos

Múltiples vulnerabilidades en HPE Smart Update Manager

Fecha de publicación: 03/06/2019

Importancia: Crítica

Recursos afectados:

- HPE Smart Update Manager (SUM) versiones anteriores a la 8.4

Descripción:

HPE ha publicado dos vulnerabilidades, de tipo escalada de privilegios locales sin autorización y acceso remoto no autorizado en su producto HPE Smart Update Manager (SUM).

Solución:

- Actualizar a la versión 8.4 o superior

Detalle:

- Una vulnerabilidad en HPE Smart Update Manager (SUM) podría permitir el acceso remoto no autorizado. Se ha reservado el identificador CVE-2019-11988 para esta vulnerabilidad.
- Una vulnerabilidad en HPE Smart Update Manager (SUM) podría permitir una escalada de privilegios locales sin autorización. Se ha reservado el identificador CVE-2019-11987 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Intelligent Operations Center de IBM

Fecha de publicación: 03/06/2019

Importancia: Alta

Recursos afectados:

- IBM® Intelligent Operations Center, versiones desde 5.1.0 hasta 5.2.0
- IBM® Intelligent Operations Center para Emergency Management, versiones desde 5.1.0 hasta 5.1.0.6
- IBM® Water Operations para Waternamics, versiones desde 5.1.0 hasta 5.2.1.1

Descripción:

Se han publicado dos vulnerabilidades de tipo denegación de servicio y validación incorrecta de archivos en Intelligent Operations Center (IOC).

Solución:

- IBM® Intelligent Operations Center, versión 5.2.0, aplicar el *interim fix* PO08061
- IBM® Intelligent Operations Center, versiones desde 5.1.0 hasta 5.1.0.14, aplicar el *interim fix* PO08131
- IBM® Water Operations for Waternamics, versiones desde 5.1.0 hasta 5.2.1.1, aplicar el *interim fix* PO08061

Detalle:

- Una vulnerabilidad en IBM Intelligent Operations Center (IOC) permitiría a un usuario autenticado crear usuarios arbitrarios que causarían problemas en la gestión de ID y, finalmente, realizarían una ejecución de código. Se ha reservado el identificador CVE-2019-4066 para esta vulnerabilidad.
- IBM Intelligent Operations Center (IOC) contiene una vulnerabilidad que causa una validación incorrecta de los tipos de archivo, lo que permitiría a un atacante cargar contenido malicioso. Se ha reservado el identificador CVE-2019-4069 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Dell EMC OpenManage System Administrator (OMSA)

Fecha de publicación: 04/06/2019

Importancia: Crítica

Recursos afectados:

- Dell EMC OpenManage System Administrator (OMSA):
  - versiones anteriores a 9.1.0.3
  - versiones anteriores a 9.2.0.4

Descripción:

Dell ha publicado dos vulnerabilidades: una de severidad crítica, del tipo manipulación de parámetros web; y otra de severidad alta, que consiste en una inyección XXE (XML External Entity).

Solución:

Dell recomienda actualizar el producto desde su centro de descargas a una de las siguientes versiones:

- 9.1.0.3 o posterior
- 9.2.0.4 o posterior
- 9.3.0 o posterior

Detalle:

- Una vulnerabilidad de inyección XXE (XML External Entity) podría permitir a un atacante remoto no autenticado leer archivos arbitrarios del servidor al proporcionar definiciones de tipo de documento (DTD), especialmente diseñadas en una solicitud XML. Se ha reservado el identificador CVE-2019-3722 para esta vulnerabilidad.
- Una vulnerabilidad de manipulación de parámetros web podría permitir a un atacante remoto no autenticado manipular los parámetros de las solicitudes web a OMSA y crear archivos arbitrarios con contenido vacío o eliminar contenido de cualquier archivo existente. Esto es debido a una validación inadecuada de los parámetros de entrada. Se ha reservado el identificador CVE-2019-3723 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Evasión de autenticación en IBM PureApplication System

Fecha de publicación: 04/06/2019

Importancia: Alta

Recursos afectados:

- IBM PureApplication System versiones:
  - 2.2.3.0
  - 2.2.3.1
  - 2.2.3.2
  - 2.2.4.0
  - 2.2.5.0
  - 2.2.5.1
  - 2.2.5.2
  - 2.2.5.3

Descripción:

IBM ha publicado una vulnerabilidad que afecta a su producto PureApplication System y que podría permitir obtener acceso de administrador.

Solución:

- Actualizar a IBM PureApplication System V2.2.6.0

Detalle:

- IBM Pure Application System podría permitir a un usuario autenticado con acceso local eludir la autenticación y obtener acceso como administrador. Se ha reservado el identificador CVE-2019-4241 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad en Jazz for Service Management (JazzSM) de IBM

Fecha de publicación: 05/06/2019

Importancia: Alta

Recursos afectados:

- Jazz for Service Management (JazzSM), versiones 1.1.3 - 1.1.3.2

Descripción:

IBM ha publicado una vulnerabilidad que afecta a su producto Jazz for Service Management (JazzSM) que podría permitir a un atacante remoto realizar ataques de *phishing*, utilizando un ataque de redireccionamiento abierto.

Solución:

- Aplicar el parche Install 1.1.3-TIV-JazzSM-multi-FP003

Detalle:

- IBM Jazz for Service Management podría permitir a un atacante remoto realizar ataques de *phishing*, utilizando un ataque de redireccionamiento abierto. Al persuadir a una víctima para que visite un sitio web especialmente diseñado, un atacante remoto podría falsificar la URL mostrada y redirigir al usuario a un sitio web malicioso en el que parece confiar. Esto podría permitirle obtener información sensible o realizar nuevos ataques contra la víctima. Se ha reservado el identificador CVE-2019-4201 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidades SQLi y CSRF en phpMyAdmin

Fecha de publicación: 05/06/2019

Importancia: Crítica

Recursos afectados:

- Las versiones de phpMyAdmin anteriores a 4.8.6 (CVE-2019-11768)
- Todas las versiones de phpMyAdmin anteriores a 4.9.0, al menos desde la versión 4.0 (CVE-2019-12616)

Descripción:

Se han encontrado dos vulnerabilidades una de ellas crítica en phpMyAdmin:

- William Desportes, miembro del equipo de phpMyAdmin, ha reportado una vulnerabilidad del tipo Inyección de SQL en la función Designer.
- Mauro Tempesta encontró una vulnerabilidad calificada como crítica del tipo CSRF (Cross-Site Request Forgery o falsificación de petición en sitios cruzados) en el formulario de inicio de sesión.

Solución:

Se recomienda actualizar el producto o aplicar los parches, respectivamente:

- Actualice a phpMyAdmin 4.8.6 o posterior o aplique el parche para la vulnerabilidad de tipo inyección SQL.
- Actualice a phpMyAdmin 4.9.0 o posterior o aplique el parche para la vulnerabilidad de tipo CSRF.

Detalle:

- La vulnerabilidad de inyección SQL permite utilizar un nombre de base de datos especialmente diseñado para desencadenar un ataque de este tipo. Se ha asignado el CVE-2019-11768 a esta vulnerabilidad.
- La vulnerabilidad de CSRF permite a un atacante engañar al usuario, por ejemplo a través de una etiqueta < img > rota en el formulario que apunta a la base de datos phpMyAdmin de la víctima, el atacante podría entregar una carga útil o payload (como una instrucción INSERT o DELETE específica). Se ha asignado el CVE-2019-12616 a esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

DoS y ejecución remota de código en varios productos de Cisco

Fecha de publicación: 06/06/2019

Importancia: Alta

Recursos afectados:

- Expressway Series configurado para acceso móvil y remoto con IM&P Service, versiones desde X8.1 hasta X12.5.2
- TelePresence VCS configurado para acceso móvil y remoto con IM&P Service, versiones desde X8.1 hasta X12.5.2
- Unified Communications Manager IM&P Service, versiones:
  - 10.5(2)
  - 11.5(1)
  - 12.0(1)
- Cisco Industrial Network Director, versiones anteriores a 1.6.0

Descripción:

Cisco ha publicado una vulnerabilidad de denegación de servicio y otra de ejecución arbitraria de código que afectan a varios de sus productos.

Solución:

Cisco ha publicado diversas actualizaciones en función del producto afectado, disponibles en su centro de descargas.

- Expressway Series configurada para acceso móvil y remoto con IM&P Service, actualizar a la versión X12.5.3 o superior.
- TelePresence VCS configurada para acceso móvil y remoto con IM&P Service, actualizar a la versión X12.5.3 o superior.
- Unified Communications Manager IM&P Service:
  - para la versión 10.5(2), actualizar a 11.5(1) SU6 o 12.5(1)
  - para la versión 11.5(1), actualizar a 11.5(1) SU6
  - para la versión 12.0(1), actualizar a 12.5(1)
- Cisco Industrial Network Director, actualizar a la versión 1.6.0 o superior.

Detalle:

- Un atacante remoto podría enviar una solicitud de autenticación malformada a *Extensible Messaging and Presence Protocol* (XMPP), pudiendo provocar un reinicio inesperado del servicio de autenticación y causar un condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2019-1845 para esta vulnerabilidad.
- Una validación incorrecta de los archivos cargados en la aplicación podría permitir a un atacante autenticado con privilegios de administrador cargar un archivo arbitrario y ejecutar código. Se ha asignado el identificador CVE-2019-1861 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 06/06/2019

Importancia: Alta

Recursos afectados:

- VMware Tools en Windows versión 10.x
- VMware Workstation Pro / Player en Linux versión 15.x

Descripción:

VMware ha publicado una vulnerabilidad de lectura fuera de límites en VMware Tools y otra de uso de memoria después de liberación en Workstation.

Solución:

- VMware Tools actualizar a la versión 10.3.10
- Workstation Pro / Player actualizar a la versión 15.1.0

Detalle:

- Una vulnerabilidad de lectura fuera de límites en el controlador vm3dmp, que se instala con vmtools en los equipos invitados de Windows, podría permitir a un atacante local sin acceso como administrador filtrar información del kernel o crear un ataque de denegación de servicio en el mismo equipo invitado de Windows. Se ha reservado el identificador CVE-2019-5522 para esta vulnerabilidad.
- La vulnerabilidad de uso de memoria después de la liberación en VMware Workstation podría permitir a un atacante, con privilegios de usuario en la máquina invitada, ejecutar código en el host Linux donde está instalada la estación de trabajo. Se ha reservado el identificador CVE-2019-5525 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Actualización de seguridad de SAP de junio de 2019

Fecha de publicación: 12/06/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5
- Solution Manager, versión 7.2
- SAP E-Commerce (Business-to-Consumer application), versiones: SAP-CRMJAV, SAP-CRMWEB, SAP-SHRWEB, SAP-SHRJAV, SAP-CRMAPP, SAP-SHRAPP 7.30, 7.31, 7.32, 7.33, 7.54
- SAP R/3 Enterprise Application, versiones: EA-APPL 600, 602, 603, 604, 605, 606, 616, 617
- SAP BusinessObjects Business Intelligence Platform (Administration Console), versiones 4.2, 4.3
- SAP NetWeaver Process Integration (PI Integration Builder Web UI), versiones: SAP_XIESR: 7.10 hasta 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; SAP_XITOOL: 7.10 hasta 7.11, 7.30, 7.31, 7.40, 7.50, SAP_XIPCK 7.10 hasta 7.11, 7.20, 7.3
- SAP Work Manager and SAP Inventory Manager, versiones SAP Work Manager 6.3.0, 6.4.0, 6.5
- SAP NetWeaver AS ABAP Platform, 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 7.21, 7.45, 7.49, 7.53, 7.73
- SAP NetWeaver Process Integration, versiones SAP_XIESR: 7.10 hasta 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; SAP_XITOOL: 7.10 hasta 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP HANA Extended Application Services (advanced model), versión 1
- SAP Enterprise Financial Services, versiones SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; EA-FINSERV 1.10, 2.0, 5.0,

6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0; Bank/CFM 4.63_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.
- Para solucionar la vulnerabilidad de severidad alta, se recomienda revisar la nota del fabricante, donde se detallan varios pasos manuales que incluyen no sólo cómo instalar el componente de software que la soluciona, sino también las dependencias de otras notas de seguridad de SAP que se deben aplicar en primer lugar y, por último, cómo realizar pasos manuales para proteger y cifrar correctamente las credenciales.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 11 notas de seguridad y 3 actualizaciones, siendo 1 de ellas de severidad crítica, 1 alta, 11 medias y 1 baja.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 5 vulnerabilidades de falta de verificación de autorización.
- 5 vulnerabilidades de divulgación de información.
- 1 vulnerabilidad de escalada de privilegios.
- 2 vulnerabilidades de otro tipo.

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

- Cuando SAP Business Client se está ejecutando en un Chromium obsoleto, un atacante podría conseguir el acceso a uno de sus usuarios para ejecutar código Javascript malicioso. El impacto real depende de qué vulnerabilidad de Chromium está siendo explotada.

- Una vulnerabilidad podría permitir a un atacante obtener credenciales de usuario válidas y la capacidad de crear cuentas de usuario privilegiadas, lo que supone un alto impacto en la confidencialidad. Se ha asignado el identificador CVE-2019-0291 para esta vulnerabilidad de severidad alta.

Los identificadores asignados para el resto de vulnerabilidades son: CVE-2019-0308, CVE-2019-0311, CVE-2019-0303, CVE-2019-0315, CVE-2019-0314, CVE-2019-0304, CVE-2018-0312, CVE-2019-0316, CVE-2019-0305, CVE-2019-0306, CVE-2019-2484 y CVE-2019-0307.

Etiquetas: Actualización, SAP, Vulnerabilidad

Boletín de seguridad de Microsoft de junio de 2019

Fecha de publicación: 12/06/2019

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player
- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- Microsoft Office y Microsoft Office Services y Web Apps
- ChakraCore
- Skype para Business y Microsoft Lync
- Microsoft Exchange Server
- Azure

Descripción:

La publicación de actualizaciones de seguridad de Microsoft de este mes consta de 87 vulnerabilidades, 21 clasificadas como críticas y 66 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:

- Ejecución remota de código.
- Divulgación de información.
- Elevación de privilegios.
- Denegación de servicio.
- Evasión de seguridad.
- Suplantación.
- Falsificación.

Etiquetas: Actualización, Microsoft, Navegador, Windows

Múltiples vulnerabilidades en productos Intel

Fecha de publicación: 12/06/2019

Importancia: Alta

Recursos afectados:

- Intel® Accelerated Storage Manager en Intel® RSTe, versiones anteriores a 5.5.0.2015
- Intel® RAID Web Console 3 para Windows, versión 4.186 y anteriores
- Intel® NUC Kit, consultar el apartado referencias para ver las versiones afectadas
- Intel® Compute Card, consultar el apartado referencias para ver las versiones afectadas
- Intel® Compute Stick, consultar el apartado referencias para ver las versiones afectadas
- Open CIT y OpenAttestation, todas las versiones
- Intel® Omni-Path Fabric Manager GUI, versiones anteriores a 10.9.2.1.1
- Intel® PROSet/Wireless WiFi Software, versiones anteriores a 21.10 para Microsoft Windows 7, 8.1 y 10
- Intel® Turbo Boost Max Technology 3.0 driver, versión 1.0.0.1035 y anteriores
- Intel® SGX Linux client driver, versiones anteriores a 2.5
- Intel® SGX DCAP Linux driver, versiones anteriores a 1.1
- ITE Tech* Consumer Infrared Driver para Windows 10, versiones anteriores a 5.4.3.0
- Intel® Chipset Device Software (INF Update Utility), versiones anteriores a 10.1.1.45

Descripción:

Intel ha publicado múltiples vulnerabilidades que afectan a varios de sus productos.

Solución:

- Actualizar a la última versión de producto afectado en el centro de descarga de software de Intel.

Detalle:

Las vulnerabilidades de criticidad alta son:

- Una vulnerabilidad de tipo Reflected XSS en la interfaz web de Intel® Accelerated Storage Manager para Intel® RSTe, podría permitir a un usuario no autenticado causar una condición de denegación de servicio a través de un acceso por red. Se ha reservado el identificador CVE-2019-0130 para esta vulnerabilidad.
- El *firmware* de Intel® NUC contiene múltiples vulnerabilidades que podrían permitir a un atacante la escalada de privilegios, provocar una condición de denegación de servicio y la divulgación de información. Se han reservado los identificadores CVE-2019-11123, CVE-2019-11124, CVE-2019-11125, CVE-2019-11126, CVE-2019-11127, CVE-2019-11128 y CVE-2019-11129.
- Una validación de sesión insuficiente en la API de servicio para Intel® RWC3 podría permitir a un atacante no autenticado habilitar una escalada de privilegios a través de un acceso por red. Se ha reservado el identificador CVE-2019-11119 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los identificadores CVE-2019-0175, CVE-2019-0177, CVE-2019-0178, CVE-2019-0179, CVE-2019-0180, CVE-2019-0181, CVE-2019-0182, CVE-2019-0183, CVE-2019-11092, CVE-2019-11117, CVE-2019-0136, CVE-2019-0164, CVE-2019-0157, CVE-2018-3702, CVE-2019-0128 y CVE-2019-0174.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de Joomla!

Fecha de publicación: 12/06/2019

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones desde 3.6.0 hasta 3.9.6.

Descripción:

Joomla! ha publicado dos nuevas versiones, la 3.9.8 y la 3.9.7, incluyendo en esta última la solución de tres vulnerabilidades de criticidad baja en su núcleo.

Solución:

Actualizar a la última versión disponible en su página web, la versión 3.9.8.

Detalle:

Las vulnerabilidades corregidas en la versión 3.9.7 son:

- Vulnerabilidad de inyección de datos CSV en la exportación del componente "com_actionslogs".
- Vulnerabilidad de tipo XSS en el campo "subform" al carecer de una suficiente validación de entrada.
- Vulnerabilidad por un incorrecto uso de los controles de acceso y ACL que permite manipular el componente "com_joomlaupdate" por usuarios que no son administradores.

Etiquetas: Actualización, CMS, Vulnerabilidad

Cross-Site Request Forgery en Cisco IOS XE Software Web

Fecha de publicación: 13/06/2019

Importancia: Alta

Recursos afectados:

Productos Cisco IOS XE Software con la característica HTTP Server habilitada.

Descripción:

Cisco ha publicado una vulnerabilidad que afecta a la interfaz web de usuario por la que un atacante remoto no autenticado podría realizar un ataque Cross-Site Request Forgery (CSRF).

Solución:

Cisco no ha publicado ninguna solución al respecto. Como medida de mitigación recomienda desactivar la característica HTTP Server mediante los comandos "*no ip http server*" o "*no ip http secure-server*".

Detalle:

Una protección insuficiente ante ataques de tipo CSRF podría permitir a un atacante aprovechar esta vulnerabilidad si persuade a un usuario de la interfaz para que acceda a un enlace malicioso. Esto le permitiría realizar acciones arbitrarias con el mismo nivel de privilegios que el usuario afectado, alterar la configuración, ejecutar comandos o reiniciar un dispositivo. Se ha reservado el identificador CVE-2019-1904 para esta vulnerabilidad.

Etiquetas: 0day, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 17/06/2019

Importancia: Alta

Recursos afectados:

- IBM InfoSphere Information:
  - Server, versiones 11.3, 11.5 y 11.7;
  - Governance Catalog, versiones 11.3, 11.5 y 11.7;
  - Server en Cloud, versiones 11.5 y 11.7;
  - Server Business Glossary, versión 9.1;
  - Server Metadata Workbench, versión 9.1.
- IBM Tivoli Netcool Impact, versiones desde 7.1.0.0 hasta 7.1.0.15.

Descripción:

IBM ha reportado dos vulnerabilidades de tipo inyección XXE (*XML External Entity*) y ejecución remota de código en sus productos IBM InfoSphere Information Server e IBM Tivoli Netcool Impact, respectivamente.

Solución:

- InfoSphere Information Server:
  - Para la versión 11.7, actualizar a las versiones 11.7.1.0 y 11.7.1.0 Enterprise Edition;
  - Para la versión 11.5, actualizar a las versiones 11.5.0.2 y 11.5 Service Pack 5, y aplicar los parches de seguridad XMETA e istool;
  - Para la versión 11.3, actualizar a la versión 11.3.1.2, y aplicar los parches de seguridad XMETA e istool.
- InfoSphere Information Governance Catalog:
  - Para la versión 11.5, aplicar el parche de seguridad;
  - Para la versión 11.3, aplicar el parche de seguridad.
- Business Glossary y Metadata Workbench: actualizar a una nueva versión.
- IBM Tivoli Netcool Impact 7.1.0: aplicar el *fix pack* 16.

Detalle:

- IBM InfoSphere Information Server es vulnerable a un ataque de inyección XXE (*XML External Entity*) al procesar datos XML. Un atacante remoto podría explotar esta vulnerabilidad para exponer información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2018-1845 para esta vulnerabilidad.
- IBM Tivoli Netcool permite la ejecución remota de comandos por parte de usuarios con bajo nivel de privilegios. Esta vulnerabilidad posibilita la ejecución de código arbitrario en el sistema, pudiendo tomar el control del mismo. Se ha reservado el identificador CVE-2019-4103 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en routers Netgear

Fecha de publicación: 17/06/2019

Importancia: Alta

Recursos afectados:

Wireless AC Router Nighthawk, modelos:

- R7900, ejecutando una versión de *firmware* anterior a la versión 1.0.3.14_10.0.40_BETA.
- R8000, ejecutando una versión de *firmware* anterior a la versión 1.0.4.38_10.1.59_BETA.

Descripción:

Cisco Talos ha descubierto dos vulnerabilidades de criticidad alta en el *firmware* para KCodes NetUSB de NETGEAR.

Solución:

NETGEAR ha publicado dos actualizaciones que solucionan las vulnerabilidades:

- R7900, versión de firmware 1.0.3.14 - Hot Fix;
- R8000, versión de firmware 1.0.4.38 - Hot Fix.

Detalle:

Las vulnerabilidades encontradas podrían permitir a un atacante remoto revelar información no autenticada del *kernel* y lectura arbitraría de memoria. Se han reservado los identificadores CVE-2019-5016 y CVE-2019-5017 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de control de acceso inadecuado en AppDNA de Citrix

Fecha de publicación: 18/06/2019

Importancia: Alta

Recursos afectados:

AppDNA, versión 7.18 y anteriores.

Descripción:

Citrix ha identificado una vulnerabilidad de control de acceso inadecuado en su producto AppDNA.

Solución:

Citrix recomienda a los clientes que actualicen AppDNA a las versiones 7 1906.1.0.0.472 y superiores y que configuren IIS (*Internet Information Services*) como se describe en la documentación del producto.

Detalle:

Se ha identificado una vulnerabilidad en AppDNA que daría lugar a que los controles de acceso no se apliquen al acceder a la consola web, lo que permitiría la escalada de privilegios y la ejecución remota de código. Se ha reservado el identificador CVE-2019-12292 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades de denegación de servicio basadas en TCP en los Kernel de Linux y FreeBSD

Fecha de publicación: 18/06/2019

Importancia: Alta

Recursos afectados:

- Versiones del Kernel de Linux:
  - SACK Panic: afecta a versiones posteriores o iguales a la versión 2.6.29;
  - SACK Slowness: anteriores a la versión 4.15;
  - Consumo excesivo de recursos: todas las versiones.
- Versiones de FreeBSD 12 que utilicen la pila RACK TCP (SACK Slowness).

Descripción:

Investigadores de Netflix han descubierto cuatro vulnerabilidades, una de criticidad alta y tres de criticidad media. Estas vulnerabilidades son debidas a las capacidades del tamaño máximo o mínimo de segmento (MSS) en los paquetes TCP, y el reconocimiento selectivo de TCP (TCP SACK). Un atacante remoto podría explotar estas vulnerabilidades para generar una condición de denegación de servicio.

Solución:

- Para sistemas operativos Linux se han publicado actualizaciones en las principales distribuciones que solucionan las vulnerabilidades:
  - Debian: instalar los paquetes de actualización de seguridad DSA-4465-1;
  - Ubuntu: instalar los paquetes de las actualizaciones de seguridad USN-4017-1 y USN-4017-2;
  - RedHat: instalar los paquetes de actualización disponibles en los diferentes avisos publicados;
  - Para el sistema operativo SUSE todavía no se han publicado parches, pero se ha informado que se proveerán los correspondientes a las distribuciones soportadas;
- Para AWS, ha informado de las siguientes actualizaciones.
- Para sistmeas operativos FreeBSD 12 no hay parche oficial, los investigadores de Netflix proponen las siguientes soluciones provisionales:
  - Aplicar el parche split_limit.patch y fijar el sysctl de *net.inet.tcp.rack.split_limit* a un valor razonable para limitar el tamaño de la tabla SACK;
  - Deshabilitar temporalmente la pila TCP RACK.

Detalle:

La vulnerabilidad de criticidad alta es debida a una secuencia de SACKs modificados que podrían desencadenar un desbordamiento de enteros, pudiendo generar un *kernel panic*. Se ha reservado el identificador CVE-2019-11477 para esta vulnerabilidad.

Al resto de vulnerabilidades de criticidad media se les han reservado los identificadores CVE-2019-11478, CVE-2019-5599 y CVE-2019-11479 para estas vulnerabilidades.

Etiquetas: Actualización, Comunicaciones, Linux, Vulnerabilidad

---

Vulnerabilidad de ejecución remota de código en Oracle WebLogic Server

Fecha de publicación: 19/06/2019

Importancia: Crítica

Recursos afectados:

Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0 y 12.2.1.3.0.

Descripción:

Oracle ha publicado una vulnerabilidad de severidad crítica que permite la ejecución remota de código en su producto Oracle WebLogic Server.

Solución:

Oracle ha puesto a disposición de los usuarios registrados un enlace para acceder a la documentación que contiene información sobre la disponibilidad de parches e instrucciones de instalación.

Detalle:

Una vulnerabilidad de deserialización, a través de XMLDecoder, en Oracle WebLogic Server, podría permitir a un atacante remoto y sin autenticación la ejecución de código. Se ha asignado el identificador CVE-2019-2729 para esta vulnerabilidad.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 20/06/2019

Importancia: Crítica

Recursos afectados:

- Los siguientes productos de Cisco que ejecuten una versión de Cisco SD-WAN Solution anterior a la 18.3.6, 18.4.1 y 19.1.0:
  - 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,
  - vSmart Controller Software.
- Cisco DNA Center Software, versiones anteriores a la 1.3.
- Los siguientes productos de Cisco que ejecuten una versión vulnerable de Cisco TelePresence TC o Cisco TelePresence CE software:
  - Cisco TelePresence Integrator C Series,
  - Cisco TelePresence EX Series,
  - Cisco TelePresence MX Series,
  - Cisco TelePresence SX Series,
  - Cisco Webex Room Series.
- Los siguiente productos de Cisco que ejecuten una versión vulnerable de Cisco StarOS operating system:
  - Cisco Virtualized Packet Core-Single Instance (VPC-SI),
  - Cisco Virtualized Packet Core-Distributed Instance (VPC-DI).
- Cisco vManage Network Management Software ejecutando una versión de Cisco SD-WAN Solution anterior a la 18.4.0.
- RV110W Wireless-N VPN Firewall, versiones anteriores a la 1.2.2.4.
- RV130W Wireless-N Multifunction VPN Router, versiones anteriores a la 1.0.3.51.
- RV215W Wireless-N VPN Router, versiones anteriores a la 1.3.1.4.
- Cisco Prime Service Catalog Software, versiones anteriores a la 12.1 Cumulative patch versión 10.
- Cisco Meeting Server deployments que ejecute versiones anteriores a la 2.2.14 y la 2.3.8.

Descripción:

Cisco ha publicado múltiples vulnerabilidades que podrían permitir a un atacante escalar privilegios, evadir la autenticación, ejecutar código remoto, denegar el servicio o llevar a cabo ataques *cross-site request forgery* (CSRF) en los productos afectados.

Solución:

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

Detalle:

Las vulnerabilidades de severidad crítica son:

- Un cumplimiento insuficiente en la autorización de los CLI de Cisco SD-WAN Solution podría permitir a un atacante autenticarse en el dispositivo y ejecutar comandos para conseguir escalar privilegios para realizar cambios en la configuración del sistema como usuario root. Se ha asignado el identificador CVE-2019-1625 para esta vulnerabilidad.
- Una restricción de acceso insuficiente a los puertos necesarios para el funcionamiento del sistema de Cisco Digital Network Architecture (DNA) Center podría permitir a un atacante conectar un dispositivo de red no autorizado a la subred designada para los servicios del clúster y acceder a servicios internos que no están protegidos frente a accesos externos. Se ha asignado el identificador CVE-2019-1848 para esta vulnerabilidad.

Para el resto de vulnerabilidades de severidad alta, se han asignado los siguientes identificadores: CVE-2019-1878, CVE-2019-1869, CVE-2019-1626, CVE-2019-1624, CVE-2019-1843, CVE-2019-1874, CVE-2019-1623.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de denegación de servicio en Apache Tomcat

Fecha de publicación: 21/06/2019

Importancia: Alta

Recursos afectados:

- Apache Tomcat®, versiones:
  - Desde la 8.5.0 hasta 8.5.40;
  - Desde la 9.0.0.M1 hasta 9.0.19.

Descripción:

Apache ha publicado una corrección para una actualización anterior, incompleta, de la vulnerabilidad con identificador CVE-2019-0199 que podría permitir a un atacante el agotamiento de los hilos y la denegación del servicio (DoS).

Solución:

- Actualizar a la versión 8.5.41 o superior.
- Actualizar a la versión 9.0.20 o superior.

Detalle:

- Mediante esta actualización se corrige una solución incompleta para el agotamiento de la ventana de conexión HTTP/2 durante la escritura. Al no enviar mensajes WINDOW_UPDATE para la ventana de conexión (stream 0), los clientes podrían hacer que los hilos del lado del servidor se bloquearan, provocando una denegación de servicio. Se ha reservado el identificador CVE-2019-10072 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades en productos Liferay

Fecha de publicación: 26/06/2019

Importancia: Crítica

Recursos afectados:

- Liferay Portal 7.1 CE GA3 y versiones anteriores sin soporte.

Descripción:

Liferay ha publicado múltiples vulnerabilidades, una de severidad crítica y cinco de severidad alta, que podrían permitir acceder a información sensible, inyectar código u obtener privilegios indebidos.

Solución:

- Actualizar a Liferay Portal 7.1 CE GA4 (7.1.3) o posterior.

Detalle:

La vulnerabilidad de severidad crítica se refiere a:

- El producto afectado es vulnerable a Server Side Request Forgery (SSRF) a través del proveedor de datos DDM REST, que podría permitir a un atacante acceder a información confidencial.

El resto de ellas, de severidad alta, son:

- Los hashes de las contraseñas y las respuestas al recordatorio de la contraseña, pueden aparecer en los registros si se produce un error en la base de datos.
- Múltiples vulnerabilidades de XSS, podrían permitir a un atacante remoto inyectar scripts web o HTML arbitrarios en una página.
- Vulnerabilidad de salto de directorio en la sección de encuestas.
- Algunos permisos pueden estar seleccionados por defecto. Esto puede provocar que algunos usuarios reciban permisos indebidos de manera involuntaria.
- La emisión de permisos múltiples podría permitir a los usuarios realizar acciones no autorizadas.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Data Center Network Manager de Cisco

Fecha de publicación: 27/06/2019

Importancia: Crítica

Recursos afectados:

- Cisco Data Center Network Manager (DCNM) versiones de software anteriores a 11.1(1).

Descripción:

El investigador independiente de seguridad, Pedro Ribeiro, a través del programa de reporte de vulnerabilidades iDefense, ha detectado dos vulnerabilidades de severidad crítica y una de severidad alta. Un atacante remoto sin autenticación podría subir archivos arbitrarios, omitir la autenticación, realizar acciones arbitrarias con privilegios de administración u obtener acceso a información sensible en el dispositivo afectado.

Solución:

- Actualizar Data Center Network Manager a la versión 11.2(1) o posterior.

Detalle:

- Una vulnerabilidad de severidad crítica se debe a una gestión incorrecta de sesión. Un atacante remoto, sin autenticación, podría realizar una petición HTTP, específicamente creada, para obtener acceso al dispositivo con privilegios de administración. Se ha asignado el identificador CVE-2019-1619 para esta vulnerabilidad.
- Una vulnerabilidad de severidad crítica se debe a unos ajustes de permisos incorrectos. Un atacante remoto, sin autenticación, podría enviar datos especialmente creados para modificar archivos y ejecutar código arbitrario con privilegios de *root*. Se ha asignado el identificador CVE-2019-1620 para esta vulnerabilidad.
- La vulnerabilidad de severidad alta se debe a unos ajustes de permisos incorrectos. Un atacante remoto, sin autenticación, podría conectarse a la interfaz web de gestión y, de este modo, descargar archivos arbitrarios del dispositivo. Se ha asignado el identificador CVE-2019-1621 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en la familia Unity de Dell EMC

Fecha de publicación: 28/06/2019

Importancia: Alta

Recursos afectados:

- Dell EMC Unity Operating Environment (OE) versiones anteriores a la 5.0.0.0.5.116;
- Dell EMC UnityVSA Operating Environment (OE) versiones anteriores a la 5.0.0.0.5.116.

Descripción:

Dell EMC Unity ha publicado múltiples vulnerabilidades que pueden poner en peligro el sistema afectado.

Solución:

Actualizar a las siguientes versiones:

- Dell EMC Unity Operating Environment (OE) versión 5.0.0.0.5.116;
- Dell EMC UnityVSA Operating Environment (OE) versión 5.0.0.0.5.116.

Detalle:

- Una vulnerabilidad de autorización inadecuada en la configuración de cuotas del servidor NAS podría permitir, a un *Unisphere Operator* autenticado remotamente, editar la configuración de cuotas de otros usuarios. Se ha reservado el identificador CVE-2019-3734 para esta vulnerabilidad.
- Las contraseñas de los usuarios de Unisphere (incluido el usuario con privilegios de administrador) se almacenan, en texto plano, en el paquete Unity Data Collection (registra los archivos para la resolución de problemas). Un atacante local autenticado con acceso al paquete de recolección de datos podría usar las contraseñas expuestas para obtener acceso con los privilegios del usuario comprometido. Se ha reservado el identificador CVE-2019-3741 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Escalada de privilegios en múltiples productos F5

Fecha de publicación: 28/06/2019

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
  - Desde la versión 14.0.0 hasta la versión 14.1.0
  - Desde la versión 13.0.0 hasta la versión 13.1.1
  - Desde la versión 12.1.0 hasta la versión 12.1.4
  - Desde la versión 11.5.2 hasta la versión 11.6.4
- Enterprise Manager versión 3.1.1
- BIG-IQ Centralized Management versiones:
  - Desde la versión 6.0.0 hasta la versión 6.1.0
  - Desde la versión 5.1.0 hasta la versión 5.4.0
- F5 iWorkflow versión 2.3.0

Descripción:

Investigadores de ING Tech Poland, ?ukasz Juszczyk y Robert Podsiad?o, han descubierto una vulnerabilidad de criticidad alta en múltiples productos de F5. Un atacante, sin autenticación, podría realizar una escalada de privilegios.

Solución:

Actualmente no se han publicado actualizaciones que solucionen la vulnerabilidad. Desde F5 recomiendan, como medida de mitigación, deshabilitar el acceso al TMOS Shell (tmsh) a todas las cuentas de usuario asociadas con el rol "*Resource Administrator*".

Detalle:

La vulnerabilidad se debe a un error en el terminal TMOS Shell (tmsh). Un atacante, sin autenticación, con la posibilidad de cargar archivos, podría realizar un escalado de privilegios y obtener una terminal con privilegios de *root*. Se ha reservado el identificador CVE-2019-6642 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad