Boletín de Septiembre de 2018

Avisos Técnicos

Múltiples vulnerabilidades en productos de HP

Fecha de publicación: 05/09/2018

Importancia: Alta

Recursos afectados:

- HPE 3PAR Service Processors - anteriores a SP-4.4.0.GA-110 (MU7)
- HP ConvergedSystem 700 Virtualization 2.0 VMware Kit - anteriores a SWFW Compatibility Matrix August 2018
- HP ConvergedSystem 700x para VMware Solution Kit - anteriores a SWFW Compatibility Matrix August 2018
- HP ConvergedSystem 700x v1.1 VMware Kit - anteriores a SWFW Compatibility Matrix August 2018

Descripción:

HPE ha publicado un boletín de seguridad en el que detalla un total de 5 vulnerabilidades, 3 de ellas de severidad alta y 2 de severidad media, que afectan a varias versiones de procesadores HPE 3PAR instalados sobre las soluciones HPE ConvergedSystem 700.

Solución:

Actualizar a la versión SP-4.4.0.GA-110 (MU7). La anterior actualización requiere que 3PAR OS esté al menos en la versión 3.2.2MU6 o superior. Los detalles y pasos a realizar pueden encontrarse en:

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03884en_us

Detalle:

Un atacante podría aprovechar las vulnerabilidades descritas en este aviso para realizar alguna de las siguientes acciones:

- Salto de directorio
- Revelación de información privilegiada
- Evasión de restricción de acceso
- Ejecución de código
- Cross-Site Request Forgery (CSRF)

Se han reservado los siguientes identificadores para las vulnerabilidades detalladas en este aviso: CVE-2018-7095, CVE-2018-7096, CVE-2018-7097, CVE-2018-7098 y CVE-2018-7099.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad en IBM WebSphere Application Server

Fecha de publicación: 06/09/2018

Importancia: Alta

Recursos afectados:

- Versiones de WebSphere Application Server: 7.0, 8.0 y 8.5.5

Descripción:

Se ha identificado una vulnerabilidad de severidad alta que podría permitir una suplantación de identidad (*spoofing*) en los productos afectados.

Solución:

La solución recomendada es aplicar el IFIX, el *Fixpack* o el PTF que contiene los APARs (*Authorized Program Analysis Report*) PI99402 para cada producto afectado tan pronto como sea posible.

Para WebSphere Application Server tradicional y WebSphere Application Server Hypervisor Edition:

- Para versiones desde la 8.5.0.0 hasta la 8.5.5.14 cuando se usa Java SE 6 existen dos opciones:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI99402.
  - Aplicar el *Fixpack* 8.5.15 o posterior (disponibilidad prevista 1Q2019).
- Para versiones desde la 8.0.0.0 hasta la 8.0.0.15 y desde la 7.0.0.0 hasta la 7.0.0.45:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI99402.

Detalle:

- Una vulnerabilidad en el software WebSphere Application Server usando *Form Login* cuando se utiliza Java SE 6 podría permitir a un atacante llevar a cabo una suplantación de identidad (*spoofing*). Esto no ocurre cuando se utilizan otras versiones de Java SE. Se ha reservado el identificador CVE-2018-1695 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 06/09/2018

Importancia: Crítica

Recursos afectados:

- RV110W Wireless-N VPN Firewall, todas las versiones
- RV130W Wireless-N Multifunction VPN Router, todas las versiones
- RV215W Wireless-N VPN Router, todas las versiones
- Servicio Cisco Umbrella
- Cisco Webex Meetings Suite (WBS31), (WBS32) y (WBS33)
- Cisco Webex Meetings
- Cisco Webex Meetings Server
- Cisco Webex Teams con versiones anteriores a 20180417-150803
- Cisco Umbrella ERC con versiones anteriores a 2.1.127
- Cisco Umbrella Roaming Module con versiones anteriores a 4.6.1098
- Routers vEdge serie 100 con versiones anteriores a 18.3.0
- Routers vEdge serie 1000 con versiones anteriores a 18.3.0
- Routers de la serie vEdge 2000 con versiones anteriores a 18.3.0
- Routers vEdge serie 5000 con versiones anteriores a 18.3.0
- vManage Network Management System con versiones anteriores a 18.3.0
- vEdge Cloud Router Platform con versiones anteriores a 18.3.0
- vSmart Controller Software con versiones anteriores a 18.3.0
- vBond Orchestrator Software con versiones anteriores a 18.3.0
- Cisco Prime Access Registrar todas las versiones y Cisco Prime Access Registrar Jumpstar versiones anteriores a 7.3.0.4 y 8.0.1.1
- Servidores UCS de la serie C que ejecutan el software Cisco IMC versión 2.0, versión 3.0 con una versión anterior a 3.0 (4d) o la versión 3.1 con una versión anterior a la 3.1 (3a)
- Servidores UCS de la serie E que ejecutan el software Cisco IMC anterior a la versión 3.2 (6)
- Plataformas del sistema de red empresarial (ENCS) de la serie 5000 que ejecutan el software Cisco IMC anterior a la versión 3.2 (6)
- Cisco Data Center Network Manager con versiones anteriores a 11.0 (1)
- Cisco Webex Player
- Cisco Tetration Analytics
- Cisco Packaged Contact Center Enterprise
- Cisco Prime Collaboration Assurance
- Cisco Network Services Orchestrator (NSO)
- Cisco Enterprise NFV Infrastructure Software (NFVIS)
- Cisco Meeting Server
- Cisco Email Security Appliance (ESA)
- Cisco Cloud Services Platform 2100
- Cisco Secure Access Control Server con versiones anteriores a 5.8 (10)

Descripción:

Cisco ha publicado 29 vulnerabilidades en varios de sus productos, siendo 2 de las mismas de severidad crítica, 13 de severidad alta y 14 de severidad media.

Solución:

Para los productos RV110W Wireless-N VPN Firewall y RV215W Wireless-N VPN Router, Cisco no publicará actualizaciones de firmware que solucionen las vulnerabilidades.

Cisco ha puesto a disposición de los usuarios diversas actualizaciones en función del producto afectado, que pueden descargarse desde:

- Panel de descarga de Software Cisco

Detalle:

Las vulnerabilidades de severidad crítica son:

- Una vulnerabilidad en la interfaz de administración web de Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, y Cisco RV215W Wireless-N VPN Router, podría permitir que un atacante remoto no autenticado provoque una denegación de servicio o ejecute código arbitrario. Esta vulnerabilidad se debe a restricciones de límite incorrectas en la entrada proporcionada por el usuario en la función de usuario invitado dentro de la interfaz web de administración. Los dispositivos únicamente son vulnerables cuando el usuario invitado de la interfaz de administración web está habilitado. Se ha reservado el identificador CVE-2018-0423 para esta vulnerabilidad.
- Una vulnerabilidad en la API Umbrella de Cisco, podría permitir a un atacante remoto autenticado ver y modificar datos en su organización o en otras organizaciones. Esto se debe a una configuración de autenticación insuficiente para la interfaz API. Se ha reservado el identificador CVE-2018-0435 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los siguientes identificadores: CVE-2018-0422, CVE-2018-0436, CVE-2018-0437 CVE-2018-0438, CVE-2018-0434, CVE-2018-0433, CVE-2018-0432, CVE-2018-0426, CVE-2018-0424, CVE-2018-0425, CVE-2018-0421, CVE-2018-0430, CVE-2018-0431, CVE-2018-0440 CVE-2018-0457, CVE-2018-0452, CVE-2018-0451, CVE-2018-0444, CVE-2018-0445, CVE-2018-0458, CVE-2018-0463, CVE-2018-0459, CVE-2018-0447, CVE-2018-0460, CVE-2018-0462, CVE-2018-0439, CVE-2018-0450, CVE-2018-0454 y CVE-2018-0414.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Ejecución remota de código en WebSphere Application Server de IBM

Fecha de publicación: 07/09/2018

Importancia: Crítica

Recursos afectados:

- IBM WebSphere Appliaction Versiones 9.0, 8.5, 8.0 y 7.0

Descripción:

IBM ha publicado una vulnerabilidad de severidad crítica que afecta a sus productos WebSphere Application y que podría permitir la ejecución remota de código.

Solución:

La solución recomendada es aplicar el IFIX, el *Fixpack* o el PTF que contiene los APARs (*Authorized Program Analysis Report*) PI95973 para cada producto afectado tan pronto como sea posible.

Para WebSphere Application Server tradicional y WebSphere Application Server Hypervisor Edition:

- Para versiones desde la 9.0.0.0 hasta la 9.0.0.9 existen dos opciones:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI95973
  - Aplicar el *Fixpack* 9.0.0.10 o posterior (disponibilidad prevista 4Q2018).
- Para versiones desde la 8.5.0.0 hasta la 8.5.5.14 existen dos opciones:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI95973
  - Aplicar el *Fixpack* 8.5.5.15 o posterior (disponibilidad prevista 1Q2019).
- Para versiones desde la 8.0.0.0 hasta la 8.0.0.15:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI95973
- Para versiones desde la 7.0.0.0 hasta la 7.0.0.45:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PI95973

Detalle:

- La vulnerabilidad podría permitir a los atacantes remotos ejecutar código Java arbitrario a través del conector SOAP con un objeto serializado de fuentes no confiables. Se ha reservado el identificador CVE-2018-1567 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en cliente ProtonVPN

Fecha de publicación: 10/09/2018

Importancia: Alta

Recursos afectados:

- Cliente de VPN ProtonVPN 1.5.1

Descripción:

Existe una vulnerabilidad de ejecución de código explotable en la funcionalidad de conexión del cliente VPN ProtonVPN 1.5.1. Un archivo de configuración OpenVPN especialmente diseñado puede causar una escalada de privilegios, lo que podría permitir la ejecución de comandos arbitrarios con los privilegios del sistema.

Solución:

Esta vulnerabilidad fue reportada por el equipo en julio y el parche ha sido incluido en una actualización del 3 de septiembre. Se recomienda actualizar los clientes VPN a la versión actual.

Detalle:

El investigador Paul Rascagneres de Cisco Talos, ha descubierto que si se modifica el archivo de configuración de OpenVPN y se agrega el parámetro *up* y a continuación la ruta de ejecución de un programa cualquiera, el programa se ejecutará con privilegios de sistema. Se ha reservado el identificador CVE-2018-4010 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en cliente

NordVPN

Fecha de publicación: 10/09/2018

Importancia: Alta

Recursos afectados:

- Cliente de VPN NordVPN 6.14.28.0

Descripción:

Existe una vulnerabilidad de ejecución de código explotable en la funcionalidad de conexión del cliente VPN NordVPN 6.14.28.0. Un archivo de configuración OpenVPN especialmente diseñado podría causar una escalada de privilegios, lo que podría permitir la ejecución de comandos arbitrarios con los privilegios del sistema.

Solución:

Un parche ha sido incluido en la actualización del cliente VPN el 8 de agosto. Se recomienda actualizar los clientes VPN a la versión actual.

Detalle:

El investigador Paul Rascagneres de Cisco Talos, ha descubierto que si se modifica el archivo de configuración de OpenVPN y se agrega el parámetro *up* y a continuación la ruta de ejecución de un programa cualquiera, el programa se ejecutará con privilegios de sistema. Se ha reservado el identificador CVE-2018-3952 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 10/09/2018

Importancia: Crítica

Recursos afectados:

- Intelligent Management Center

Descripción:

El investigador Sztivi ha descubierto 9 vulnerabilidades de severidad crítica en productos HPE que podrían permitir a un atacante remoto sin autenticación la ejecución de código arbitrario.

Solución:

Por el momento no existe ninguna actualización que solucione estas vulnerabilidades. Se recomienda, como medida de mitigación, restringir la interacción del servicio con máquinas de confianza mediante, por ejemplo, cortafuegos y listas blancas.

Detalle:

- Un atacante puede aprovechar las siguientes vulnerabilidades para ejecutar código arbitrario en el contexto de SYSTEM, debido a:
  - La inadecuada comprobación de los datos de entrada suministrados por el usuario en el servicio dbman, en el puerto de escucha TCP 2810 (por defecto).
  - El manejo de las peticiones de opcode 10010 en el servicio dbman, en el puerto de escucha TCP 2810 (por defecto) que permite la escritura arbitraria de archivos con datos controlados por el usuario.
  - La inadecuada validación del parámetro de nombre de usuario proporcionado al método dealInodeNotifyMsg antes de copiarlos a un búfer basado en pilas de longitud fija.
  - Un checkeo inapropiado de la longitud de los datos suministrados por el usuario dentro del descifrado de mensajes encriptados antes de copiarlos a un búfer basado en pilas de longitud fija.
  - El procesamiento del mensaje dealInodeOfflineMsg no valida adecuadamente la longitud de los datos suminstrados por el usuario antes de copiarlos a un búfer basado en pilas de longitud fija.

Etiquetas: 0day, HP, Vulnerabilidad

Boletín de seguridad de Microsoft de septiembre de 2018

Fecha de publicación: 12/09/2018

Importancia: Crítica

Recursos afectados:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- Microsoft.Data.OData
- ASP.NET

Descripción:

La publicación de actualizaciones de seguridad de Microsoft este mes consta de 60 vulnerabilidades, 17 clasificadas como críticas y 43 como importantes, siendo el resto de severidad media o baja.

Solución:

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

Detalle:

El tipo de vulnerabilidades publicadas se corresponde a las siguientes:

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

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

---

Actualización de seguridad de SAP de septiembre 2018

Fecha de publicación: 12/09/2018

Importancia: Alta

Recursos afectados:

- SAP Business Client, versión 6.5
- SAP Business One, versiones 9.2 y 9.3
- SAP NetWeaver BI, versiones 7.30,7.31,7.40,7.41 y 7.50
- SAP HANA, versiones 1.0 y 2.0
- SAP WebDynpro, versiones 7.20, 7.30, 7.31, 7.40, 7.50
- SAP NetWeaver AS Java, versiones de la 7.10 a la 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP Hybris Commerce, versiones 6.*
- SAP Plant Connectivity, versión 15.0
- SAP Adaptive Server Enterprise, versión 16.0
- SAP HCM Fiori "People Profile" (GBX01HR), versión 6.0
- SAP Mobile Platform, versión 3.0
- SAP Enterprise Financial Services, versión 6.05, 6.06, 6.16, 6.17, 6.18, 8.0
- SAP Business One Android application, versión 1.2

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 14 notas de seguridad, de las cuales 1 es una actualización de una nota de seguridad publicada con anterioridad, 3 de severidad alta, 9 de de severidad media y 1 de severidad baja.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 1 vulnerabilidad de denegación de servicio
- 3 vulnerabilidades de divulgación de información
- 3 vulnerabilidades de falta de comprobación de autorización
- 2 vulnerabilidades de Cross-Site Scripting
- 2 vulnerabilidades de incorrecta validación de XML
- 3 vulnerabilidades de otras tipologías

Las vulnerabilidades más relevantes son las siguientes:

- La vulnerabilidad de divulgación de información en SAP Business ONE y SAP HANA, podría permitir a un atacante revelar información adicional (datos del sistema, información de depuración, etc.) que ayudaría a aprender sobre un sistema y planificar otros ataques. Esto podría desembocar en la divulgación de información, escalamiento de privilegios y otros ataques. Se ha asignado el código CVE-2018-2458 para esta vulnerabilidad.

- Un atacante puede utilizar la vulnerabilidad de incorrecta validación de XML, presente en SAP BEx Web Java Runtime Export Web Service, para enviar solicitudes XML especialmente diseñadas y no autorizadas que serían procesadas por el analizador XML. El atacante obtendría acceso no autorizado al sistema de archivos del SO. Se ha asignado el código CVE-2018-2462 para esta vulnerabilidad.

- Una vulnerabilidad de falta de comprobación de autorizacion en SAP ECC Sales Support podría permitir a un atacante el acceso a un servicio sin necesidad de autorización y emplear funciones de servicio con acceso restringido. Esto puede desembocar en la divulgación de información, escalado de privilegios y otros ataques.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabildiades en productos de Intel

Fecha de publicación: 12/09/2018

Importancia: Alta

Recursos afectados:

- Intel® Data Migration Software v3.1 y anteriores
- Intel® OpenVINO™ Toolkit for Windows v2018.1.265 and earlier
- Intel® IoT Developers Kit 4.0 y anteriores
- Intel® NUC Kit, varios modelos
- Intel® Compute Card, varios modelos
- Intel® Compute Stick, varias modelos
- Intel® Centrino® Wireless-N, varios modelos
- Intel® Centrino® Advanced-N, varios modelos
- Intel® Distribution for Python 2018 versiones descargadas antes del 6 de agosto del 2018
- Intel® Extreme Tuning Utility, versiones anteriores a 6.4.1.23
- Intel® Driver & Support Assistant, versiones anteriores a 3.5.0.1
- Intel® Computing Improvement Program, versiones anteriores a 2.2.0.03942
- Intel-SA-00086 Detection Tool, versiones anteriores a 1.2.7.0
- Intel® CSME, versiones desde 11.0 hasta 11.8.50; desde 11.10 hasta 11.11.50; desde 11.20 hasta 11.21.51, Intel® Server Platform Services firmware versión 4.0 (en Purley y Bakerville only) e Intel® TXE versiones desde la 3.0 hasta 3.1.50.
- Sistemas que usen Intel® CSME con versiones de firmware anteriores a 11.0/ Intel® Server Platform Services 4.0/TXE 3.0 o que usen las versiones de firmware 11.8.55/11.11.55/11.21.55/ Intel® Server Platform Services 5.0 y superiores /TXE 3.1.55 o superiores no están afectadas por esta vulnerabilidad.
- Intel® CSME, varias versiones
- Intel® ME, varias versiones
- Intel® Trusted Execution Engine (TXE), varias versiones
- Intel® Data Center manager, versiones anteriores a 5.1
- Intel® Server Board, varias versiones
- Intel® Server Board S2600BP, S2600WF y S2600ST

Descripción:

Intel ha publicado 16 avisos de seguridad en su centro de seguridad de productos, 1 de severidad crítica, 7 de severidad alta y 8 de severidad media.

Solución:

Actualizar a la última versión de producto en https://downloadcenter.intel.com/.

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- Escalada de privilegios
- Ejecución de código con otros privilegios
- Ejecución de código arbitrario
- Revelación de información
- Denegación de servicio

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 17/09/2018

Importancia: Alta

Recursos afectados:

Se han visto afectadas las siguientes versiones, según la vulnerabilidad:

- MSA-18-0019: 3.5 hasta 3.5.1, 3.4 hasta 3.4.4, 3.3 hasta 3.3.7 y versiones anteriores sin soporte.
- MSA-18-0018: 3.5 hasta 3.5.1, 3.4 hasta 3.4.4, 3.3 hasta 3.3.7, 3.1 hasta 3.1.13 y versiones anteriores sin soporte.
- MSA-18-0017: 3.5 hasta 3.5.1, 3.4 hasta 3.4.4, 3.1 hasta 3.1.13 y versiones anteriores sin soporte.

Descripción:

Se han descubierto 3 vulnerabilidades en Moodle, una de criticidad alta y 2 de criticidad baja. Estas vulnerabilidades podrían ocasionar un XSS reflejado (o indirecto) o una inyección y ejecución de código PHP; además, se ha actualizado una librería de terceros como medida de precaución.

Solución:

Se han puesto a disposición de los usuarios las siguientes actualizaciones en función de la vulnerabilidad:

- MSA-18-0019: 3.5.2, 3.4.5 y 3.3.8.
- MSA-18-0018 y MSA-18-0017: 3.5.2, 3.4.5, 3.3.8 y 3.1.14.

Detalle:

La vulnerabilidad de criticidad alta es la siguiente:

- Al importar preguntas de prueba heredadas con el método *drag and drop into text*, un atacante podría inyectar y ejecutar código PHP en las preguntas importadas, ya sea intencionadamente o importando preguntas de una fuente no confiable.

Se han reservado los siguientes identificadores para estas vulnerabilidades: CVE-2018-14631 (MSA-18-0019), CVE-2018-1999022 (MSA-18-0018) y CVE-2018-14630 (MSA-18-0017).

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

Vulnerabilidad en BIG-IP ASM de F5

Fecha de publicación: 19/09/2018

Importancia: Media

Recursos afectados:

- BIG-IP ASM versiones comprendidas entre la 12.1.2 y la 12.1.3.6

Descripción:

F5 ha descubierto una vulnerabilidad que afecta a BIG-IP ASM, por la cual, puede dejar de aplicar las firmas de ataque despúes de activar una política de seguridad que incluye una nueva firma.

Solución:

F5 ha publicado una actualización a la versión 12.1.3.7. También recomienda actualizar las otras políticas de seguridad para hacer referencia al nuevo ID de colección de firmas.

Detalle:

El problema aparece cuando se cumplen las siguientes condiciones:

- El sistema BIG-IP ASM ejecuta versiones comprendidas entre 12.1.2 a 12.1.3.6.
- Tiene configuradas múltiples políticas de seguridad en el sistema BIG-IP ASM.
- Una de las políticas de seguridad incluye una nueva firma de ataque no incluida en otras políticas.
- Activa la política de seguridad que incluye la nueva firma.

Cuando se activa la política de seguridad, el sistema regenera la colección de firmas base con una ID incrementada. Cuando se produce este problema, solo se actualiza la política de seguridad recientemente activada para hacer referencia al nuevo ID de colección de firmas.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Cisco Webex Network Recording Player

Fecha de publicación: 20/09/2018

Importancia: Alta

Recursos afectados:

- Cisco Webex Meetings Suite (WBS32) - Webex Network Recording Player versiones anteriores a WBS32.15.10
- Cisco Webex Meetings Suite (WBS33) - Webex Network Recording Player versiones anteriores a WBS33.3
- Cisco Webex Meetings Online - Webex Network Recording Player versiones anteriores a 1.3.37
- Cisco Webex Meetings Server - Webex Network Recording Player versiones anteriores a 3.0MR2

Descripción:

Cisco ha publicado un aviso de seguridad, que incluye 3 vulnerabilidades de severidad alta, que podrían permitir a un atacante remoto la ejecución de código arbitrario en los sistemas afectados.

Solución:

Las siguientes versiones de producto solucionan las vulnerabilidades descritas en este aviso:

- Cisco Webex Meetings Suite (WBS32) - Cisco Webex Network Recording Player versiones WBS32.15.10 y posteriores
- Cisco Webex Meetings Suite (WBS33) - Cisco Webex Network Recording Player versiones WBS33.3 y posteriores
- Cisco Webex Meetings Online - Webex Network Recording Player versiones 1.3.37 y posteriores
- Cisco Webex Meetings Server - Webex Network Recording Player versiones 3.0MR2 y posteriores

Las últimas versiones del reproductor ARF están disponibles en:

http://www.webex.com/play-webex-recording.html

Detalle:

Un usuario podría ser persuadido para hacer clic en un enlace o abrir un fichero de un email malicioso, que podría permitir a un ciberdelincuente la ejecución de código arbitrario en los sistemas afectados. Se han reservado los identificadores CVE-2018-15414, CVE-2018-15421 y CVE-2018-15422 para estas vulnerabilidades.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Db2 de IBM

Fecha de publicación: 21/09/2018

Importancia: Alta

Recursos afectados:

Versiones de IBM Db2:

- V9.7.
- V10.1.
- V10.5.
- V11.1.

Descripción:

IBM ha detectado 3 vulnerabilidades de criticidad alta en Db2 que podrían permitir a un atacante local la elevación de privilegios y el desbordamiento de búfer con ejecución arbitraria de código.

También ha publicado otras vulnerabilidades en Db2 de criticidades medias o bajas. En el apartado Referencias puede encontrar más información.

Solución:

IBM ha puesto a disposición de los usuarios actualizaciones de seguridad que solucionan las vulnerabilidades en función de la versión afectada, disponibles en el siguiente enlace:

Fix Central

Detalle:

- Una vulnerabilidad en la herramienta db2licm de desbordamiento de búfer, puede dar lugar a la ejecución arbitraria de código. Se ha reservado el identificador CVE-2018-1710 para esta vulnerabilidad.
- Una vulnerabilidad en el planificador de tardeas administrativas de IBM Db2, podría permitir a un usuario local obtener privilegios debido a que permite la modificación de columnas de tareas existentes. Se ha reservado el identificador CVE-2018-1711 para esta vulnerabilidad.
- Una vulnerabilidad en GSKit afecta a IBM Spectrum Scale utilizado por Db2, podría permitir a un atacante local obtener el control del de Spectrum Scale daemon, acceder y modificar archivos en el sistema de archivos de Spectrum Scales, y posiblemente obtener privilegios de administrador en el nodo. Se ha asignado el identificador CVE-2018-1431 para esta vulnerabilidad.

Para las vulnerabilidades de severidad media o baja, se han asignado los identificadores CVE-2016-0705, CVE-2017-3732, CVE-2018-1447.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 21/09/2018

Importancia: Alta

Recursos afectados:

- HP XP7 Automation Director Software de 8.5.2-02 a antes de 8.6.1-00.
- HPE XP7 Automation Director Software de 8.5.2-02 a antes de 8.6.1-00 para los modelos 1TB 101-250TB LTU, 1TB 251-500TB LTU, 1TB Enterprise LTU, 1TB Over 500TB LTU, 1TB-day Meter LTU, Base LTU y Unlimited LTU.
- Todas las licencias de HPE XP P9000 Command View Advanced Edition Software.
- Todas los HPE XP7 Command View Advanced Edition Suite.
- HPE 3PAR Service Processors - anterior a SP-4.4.0.GA-110(MU7).
- HP ConvergedSystem 700 Virtualization 2.0 VMware Kit - anterior a SWFW Compatibility Matrix de noviembre 2017.
- HP ConvergedSystem 700x for VMware Solution Kit - anterior a SWFW Compatibility Matrix de noviembre 2017.
- HP ConvergedSystem 700x v1.1 VMware Kit - anterior a SWFW Compatibility Matrix de noviembre 2017.
- HPE enhanced Internet Usage Manager (eIUM) 9.0 FP01 - Incluyendo versiones específicas del cliente basadas en la versión 9.0 FP01.

Descripción:

Se han detectado varias vulnerabilidades en diversos productos de HPE:

- En HPE StorageWorks XP7 Automation Director podría provocar *bypass* de autenticación local y remota.
- En HPE XP P9000 Command View Advanced Edition podría provocar acceso sin autorización a información sensible, tanto local como remota.
- En HPE Command View Advanced Edition podría provocar *bypass* de restricción local y remota.
- En HPE Command View Advanced Edition usando JDK podría provocar *bypass* de autenticación local y remota.
- Múltiples vulnerabilidades en HPE ConvergedSystem 700 Solutions usando HPE 3PAR Service Processor.
- En HPE Internet Usage Manager mejorado podría provocar modificación remota de archivos arbitrarios.

Solución:

- Para HPE StorageWorks XP7 Automation Director actualizar a AutoDir version 8.6.1-00 o posteriores.
- Para HPE XP P9000 Command View Advanced Edition aplicar las actualizaciones DevMgr 8.6.1-00 y CM 8.6.1-00 (solo si REST API es usado, en caso contraio desintalar CM).
- Para HPE Command View Advanced Edition actualizar a las versiones especificadas o superiores:
    - DevMgr 8.6.0-00: desde DevMgr 8.4.0-00 o superiores, CM está también instalado con DevMgr automáticamente. Esta vulnerabilidad está corregida en DevMgr 8.6.0-00, que incluye CM 8.6.0-00. Para arreglar esta vulnerabilidad:
        - Actualizar DevMgr y CM a 8.6.1-00 o superiores.
        - Si la funcionalidad de CM no es necesaria, desinstalar CM después de haber actualizado DevMgr 8.6.0-00.
    - TSMgr 8.6.0-00
    - RepMgr 8.6.0-00
    - HGLM 8.6.0-00
    - AutoDir 8.6.0-00
    - CM 8.6.1-00: desde DevMgr 8.4.0-00 o superiores, CM está también instalado con DevMgr automáticamente. Esta vulnerabilidad está corregida en DevMgr 8.6.0-00, que incluye CM 8.6.0-00. Para arreglar esta vulnerabilidad:
        - Actualizar DevMgr y CM a 8.6.1-00 o superiores.
        - Si la funcionalidad de CM no es necesaria, desinstalar CM después de haber actualizado DevMgr 8.6.0-00.
- Para HPE Command View Advanced Edition las vulnerabilidades se resolverán en una futura versión de los productos, como solución provisional se puede cambar el JDK usado por estos productos a Oracle JDK (8u181 o superior).
- Para HPE ConvergedSystem 700 Solutions usando HPE 3PAR Service Processor seguir los pasos especificados en la web de la vulnerabilidad listada en la sección *Referencias.*
- Para HPE Internet Usage Manager mejorado se debe aplicar el último parche acumulativo eIUM90FP01XXX.YYYYMMDD-HHMM a todas las instalaciones basadas en la versión 9.0 FP01XXX, donde XXX es un identificador del cliente.

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- HPE StorageWorks XP7 Automation Director (AutoDir) versión 8.5.2-02 a anterior a la 8.6.1-00 tiene una vulnerabilidad que expuso la información de autenticación del usuario del sistema de almacenamiento. Este problema a veces se produce bajo condiciones específicas al ejecutar una plantilla de servicio. Se ha asignado el identificador CVE-2018-7108.
- Los productos HPE XP P9000 Command View Advanced Edition (CVAE) tienen una vulnerabilidad en el servidor web, que se incluye con los productos CVAE, donde se puede recuperar la información del usuario. Este software podría ser explotado para permitir el acceso no autorizado local y remoto a información confidencial. Se ha asignado el identificador CVE-2016-9877.
- HPE Command View Advanced Edition (CVAE) es vulnerable al *bypass* de restricción de acceso local y remoto. Se han asignado los identificadores CVE-2017-3736 y CVE-2017-3738.
- HPE Command View Advanced Edition (CVAE) usando JDK es vulnerable al *bypass* de autenticación de acceso local y remoto. Se han asignado los identificadores CVE-2018-2940, CVE-2018-2952 y CVE-2018-2973.
- En HPE ConvergedSystem 700 Solutions usando HPE 3PAR Service Processor las vulnerabilidades pueden explotarse localmente para permitir el cruce de directorios, la divulgación de información privilegiada y la explotación remota para permitir la omisión de restricción de acceso, la ejecución de código y Cross-Site Request Forgery (CSRF). Se han asignado los identificadores CVE-2018-7095, CVE-2018-7096, CVE-2018-7097, CVE-2018-7098 y CVE-2018-7099.
- En HPE Internet Usage Manager mejorado (eIUM) tiene un avulnerabilidad de modificación arbitraria remota de ficheros. Se ha asignado el identificador CVE-2018-7109.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad en Cisco Video Surveillance Manager

Fecha de publicación: 24/09/2018

Importancia: Crítica

Recursos afectados:

Cisco Video Surveillance preinstalado por Cisco en versiones:

- 7.10
- 7.11
- 7.11.1

Mientras se ejecute en una de las siguientes plataformas:

- CPS-UCSM4-1RU-K9
- CPS-UCSM4-2RU-K9
- KIN-UCSM5-1RU-K9
- KIN-UCSM5-2RU-K9

Descripción:

Una vulnerabilidad en el software Cisco Video Surveillance Manager (VSM) ejecutado en ciertas plataformas de Cisco Unified Computing System (UCS), podría permitir que un atacante remoto no autenticado inicie sesión en un sistema afectado mediante la cuenta *root*, con credenciales por defecto y ejecutar comandos arbitrarios.

Solución:

Cisco ha lanzado una actualización a la versión 7.12 que se puede descargar desde su página web para corregir esta vulnerabilidad.

Detalle:

Se ha descubierto una vulnerabilidad en el software Cisco Video Surveillance Manager (VSM) ejecutado en ciertas plataformas de Cisco Unified Computing System (UCS), que podría permitir a un atacante remoto no autenticado iniciar sesión en un sistema afectado mediante la cuenta *root* que tenga credenciales por defecto y ejecutar comandos arbitrarios.

Esta vulnerabilidad existe debido a que Cisco no deshabilitó la cuenta *root* antes de preinstalar el software. Las credenciales para esta cuenta no están documentadas de forma pública. Se ha reservado el identificador CVE-2018-15427 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 26/09/2018

Importancia: Alta

Recursos afectados:

- D3600, versiones anteriores a 1.0.0.76
- D6000, versiones anteriores a 1.0.0.76
- D1500, versiones anteriores a 1.0.0.27
- D500, versiones anteriores a 1.0.0.27
- D6100, versiones anteriores a 1.0.0.58
- D6200, versiones anteriores a 1.1.00.30
- D6220, versiones anteriores a 1.0.0.46
- D6400, versiones anteriores a 1.0.0.82
- D7000, versiones anteriores a 1.0.1.68
- D7000v2, versiones anteriores a 1.0.0.51
- D7800, versiones anteriores a 1.0.1.42

- D8500, versiones anteriores a 1.0.3.42
- DC112A, versiones anteriores a 1.0.0.40
- DGN2200Bv4, versiones anteriores a 1.0.0.102
- DGN2200v4, versiones anteriores a 1.0.0.102
- JNR1010v2, versiones anteriores a 1.1.0.54
- JR6150, versiones anteriores a 1.0.1.18
- JWNR2010v5, versiones anteriores a 1.1.0.54
- PR2000, versiones anteriores a 1.0.0.24
- R6020, versiones anteriores a 1.0.0.34
- R6050, versiones anteriores a 1.0.1.18
- R6080, versiones anteriores a 1.0.0.34
- R6100, versiones anteriores a 1.0.1.22
- R6120, versiones anteriores a 1.0.0.42
- R6220, versiones anteriores a 1.1.0.68
- R6250, versiones anteriores a 1.0.4.30
- R6300v2, versiones anteriores a 1.0.4.32
- R6400, versiones anteriores a1.0.1.44
- R6400v2, versiones anteriores a 1.0.2.60
- R6700, versiones anteriores a 1.0.1.48
- R6700v2, versiones anteriores a 1.2.0.24
- R6800, versiones anteriores a 1.2.0.24
- R6900, versiones anteriores a 1.0.1.48
- R6900P, versiones anteriores a 1.3.1.44
- R6900v2, versiones anteriores a 1.2.0.24
- R7000, versiones anteriores a 1.0.9.34
- R7000P, versiones anteriores a 1.3.1.44
- R7100LG, versiones anteriores a 1.0.0.48
- R7300, versiones anteriores a 1.0.0.68
- R7500, versiones anteriores a 1.0.0.124
- R7500v2, versiones anteriores a 1.0.3.38
- R7900, versiones anteriores a 1.0.2.16
- R7900P, versiones anteriores a 1.4.1.24
- R8000, versiones anteriores a 1.0.4.18
- R8000P, versiones anteriores a 1.4.1.24
- R8300, versiones anteriores a 1.0.2.122
- R8500, versiones anteriores a 1.0.2.122
- WN3000RP, versiones anteriores a 1.0.0.68
- WN3000RPv2, versiones anteriores a 1.0.0.68
- WNDR3400v3, versiones anteriores a 1.0.1.18
- WNDR3700v4, versiones anteriores a 1.0.2.102
- WNDR3700v5, versiones anteriores a 1.1.0.54
- WNDR4300v1, versiones anteriores a 1.0.2.104
- WNDR4300v2, versiones anteriores a 1.0.0.56
- WNDR4500v3, versiones anteriores a 1.0.0.56
- WNR1000v4, versiones anteriores a 1.1.0.54
- WNR2020, versiones anteriores a 1.1.0.54
- WNR2050, versiones anteriores a 1.1.0.54
- WNR3500Lv2, versiones anteriores a 1.2.0.54

Descripción:

Netgear ha publicado 2 vulnerabilidades de severidad alta que afectan a varios de sus routers, extensores wifi y bases de expansión.

Solución:

Actualizar los productos afectados a la última versión de firmware que puede encontrarse en: https://www.netgear.com/support/.

Detalle:

- Vulnerabilidad por configuración incorrecta de seguridad, afecta a los routers D3600 y D6000.
- Vulnerabilidad de revelación de información sensible, afecta al resto de productos afectados.

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 26/09/2018

Importancia: Alta

Recursos afectados:

- Arachni Scanner Plugin versión 0.9.7 y anteriores.
- Argus Notifier Plugin versión 1.0.1 y anteriores.
- Artifactory Plugin versión 2.16.1 y anteriores.
- Chatter Notifier Plugin versión 2.0.4 y anteriores.
- Config File Provider Plugin versión 3.1 y anteriores.
- Crowd 2 Integration Plugin versión 2.0.0 y anteriores.
- Dimensions Plugin versión 0.8.14 y anteriores.
- Email Extension Template Plugin versión 1.0 y anteriores.
- Git Changelog Plugin versión 2.6 y anteriores.
- HipChat Plugin versión 2.2.0 y anteriores.
- JIRA Plugin versión 3.0.1 y anteriores.
- Job Configuration History Plugin versión 2.18 y anteriores.
- JUnit Plugin versión 1.25 y anteriores.
- mesos Plugin versión 0.17.1 y anteriores.
- Metadata Plugin versión 1.1.0b y anteriores.
- Monitoring Plugin versión 1.73.1 y anteriores.
- MQ Notifier Plugin versión 1.2.6 y anteriores.
- PAM Authentication Plugin versión 1.3 y anteriores.

- Publish Over Dropbox Plugin versión 1.2.4 y anteriores.
- Rebuilder Plugin versión 1.28 y anteriores.
- SonarQube Scanner Plugin versión 2.8 y anteriores.

Descripción:

Se han publicado varias vulnerabilidades en el software de automatización y despliegue de proyectos Jenkins. Un atacante remoto podría aprovechar estas vulnerabilidades para ejecutar ataques de falsificación de petición en sitios cruzados (CSRF), inyecciones de código malicioso (XSS) tanto persistente como reflejado, enumeración de credenciales por parte de usuarios sin privilegios, falsificación de solicitudes del lado del servidor (SSRF), almacenaje de credenciales almacenadas en texto plano o acceso a cuentas sin validación apropiada.

Solución:

- Arachni Scanner Plugin debe ser actualizado a la versión 1.0.0.
- Argus Notifier Plugin debe ser actualizado a la versión 1.0.2.
- Artifactory Plugin debe ser actualizado a la versión 2.16.2.
- Chatter Notifier Plugin debe ser actualizado a la versión 2.0.5.
- Config File Provider Plugin debe ser actualizado a la versión 3.2.
- Crowd 2 Integration Plugin debe ser actualizado a la versión 2.0.1.
- Dimensions Plugin debe ser actualizado a la versión 0.8.15.
- Email Extension Template Plugin debe ser actualizado a la versión 1.1.
- Git Changelog Plugin debe ser actualizado a la versión 2.7.
- HipChat Plugin debe ser actualizado a la versión 2.2.1.
- JIRA Plugin debe ser actualizado a la versión 3.0.2.
- Job Configuration History Plugin debe ser actualizado a la versión 2.18.1.
- JUnit Plugin debe ser actualizado a la versión 1.26.
- mesos Plugin debe ser actualizado a la versión 0.18.
- Metadata Plugin aún no tiene *fix* disponible.
- Monitoring Plugin debe ser actualizado a la versión 1.74.0.
- MQ Notifier Plugin debe ser actualizado a la versión 1.2.7.
- PAM Authentication Plugin debe ser actualizado a la versión 1.4.
- Publish Over Dropbox Plugin debe ser actualizado a la versión 1.2.5.
- Rebuilder Plugin debe ser actualizado a la versión 1.29.
- SonarQube Scanner Plugin debe ser actualizado a la versión 2.8.1.

Detalle:

De todas las vulnerabilidades, solo la siguiente tiene criticidad alta:

- SECURITY-1156: La biblioteca JavaMelody incluida en Monitoring Plugin se ve afectada por una vulnerabilidad de procesamiento de XML External Entity (XXE). Esto permite al atacante enviar solicitudes elaboradas a una aplicación web para extraer información del sistema de archivos, falsificación de solicitudes del lado del servidor (SSRF) o ataques de denegación de servicio (DoS). Se ha reservado el identificador CVE-2018-15531 para esta vulnerabilidad.

También se han hecho públicas otras vulnerabilidades de criticidad media y baja con los identificadores: SECURITY-130, SECURITY-265, SECURITY-813 (CVE-2017-12197), SECURITY-845, SECURITY-938, SECURITY-948, SECURITY-972, SECURITY-984 (2), SECURITY-1011 (2), SECURITY-1013 (2), SECURITY-1029, SECURITY-1050 (2), SECURITY-1065, SECURITY-1067, SECURITY-1068, SECURITY-1075, SECURITY-1080, SECURITY-1101, SECURITY-1108, SECURITY-1122, SECURITY-1125, SECURITY-1130, SECURITY-1135, y SECURITY-1163.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 27/09/2018

Importancia: Alta

Recursos afectados:

- HPE SGF 4.2 para RHEL 6 y RHEL 7
  - E-Media SGF 4.2
  - Media SGF 4.2
- HPE SGF 4.3 para RHEL 6 y RHEL 7
  - E-Media SGF 4.3
  - Media SGF 4.3
- HPE Intelligent Management Center (iMC) anterior a iMC PLAT 7.3 E0605P04

Descripción:

Se han detectado varias vulnerabilidades en diversos productos de HPE:

- En HPE Service Governance Framework (SGF) se podría producir una divulgación remota no autorizada de información.
- En HPE Intelligent Management Center (iMC) PLAT se podría producir una ejecución remota de código.

Solución:

- Para la la vulnerabilidad de divulgación remota no autorizada de información en HPE Service Governance Framework (SGF) se debe actualizar SGF solicitando a la asistencia de HPE que proporcione el parche de seguridad disponible.
- Para la vulnerabilidad de ejecución remota de código en HPE Intelligent Management Center (iMC) PLAT se especifica que está solucionada en la versión iMC PLAT 7.3 E0605P04, y la lista de productos de red de HP que se incluyen en la actualización aparecen en la sección *Resolution* de la web.

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- Puede darse una condición de carrera con carga alta en HPE Service Governance Framework (HPE SGF) donde SGF transfirió diferentes parámetros al habilitador. Esto permite una vulnerabilidad de divulgación remota no autorizada de información. Se ha reservado el identificador CVE-2018-7110 para esta vulnerabilidad.

- Una vulnerabilidad de seguridad en HPE Intelligent Management Center (iMC) PLAT podría aprovecharse para permitir la ejecución remota de código. Se han reservado los identificadores CVE-2018-7076, CVE-2017-17485, CVE-2017-7525, CVE-2017-9096, CVE-2018-5968 y CVE-2018-7489 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad en el software EAP de TP-Link

Fecha de publicación: 27/09/2018

Importancia: Alta

Recursos afectados:

- EAP Controller versión 2.5.3 y anteriores.

Descripción:

El controlador TP-Link EAP carece de autenticación RMI y es vulnerable a los ataques de deserialización.

Solución:

Actualmente no hay una actualización disponible para el controlador EAP que aborde completamente la vulnerabilidad. Sin embargo, TP-Link recomienda tomar una serie de medidas para ayudar a mitigar y reducir el riesgo.

- Actualizar Apache Commons Collections
- Actualizar JRE de EAP a la última versión

Detalle:

El software TP-Link EAP para Linux, que permite controlar de forma remota los dispositivos de punto de acceso inalámbrico (WAP), carece de autenticación de usuario para los comandos de servicio RMI. Además, utiliza una versión obsoleta y vulnerable de Apache Commons Collections. Un atacante remoto podría implementar ataques de deserialización a través del protocolo RMI, controlar de forma remota el servidor EAP Controller y ejecutar funciones de Java o bytecode Java. Se ha asignado el identificador CVE-2015-6420 para la vulnerabilidad de Apache Commons Collections. Y se ha reservado el identificador CVE-2018-5393 para la vulnerabilidad del controlador de EAP.

Etiquetas: Actualización, Apache, Comunicaciones, Java, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 27/09/2018

Importancia: Alta

Recursos afectados:

- D3600, versiones de firmware anteriores a 1.0.0.76
- D6000, versiones de firmware anteriores a 1.0.0.76
- R6700, versiones de firmware anteriores a 1.0.1.48
- R7500, versiones de firmware anteriores a 1.0.0.124
- R7800, versiones de firmware anteriores a 1.0.2.58
- R8900, versiones de firmware anteriores a 1.0.4.2
- R9000, versiones de firmware anteriores a 1.0.4.2
- WNDR3700v4, versiones de firmware anteriores a 1.0.2.102
- WNDR4300v1, versiones de firmware anteriores a 1.0.2.104
- WNDR4300v2, versiones de firmware anteriores a 1.0.0.56
- WNDR4500v3, versiones de firmware anteriores a 1.0.0.56
- WNR2000v5 (R2000), versiones de firmware anteriores a 1.0.0.68
- R7900, versiones de firmware anteriores a 1.0.2.16
- R6900, versiones de firmware anteriores a 1.0.1.48
- R7000P, versiones de firmware anteriores a 1.3.1.44
- R6900P, versiones de firmware anteriores a 1.3.1.44
- R6250, versiones de firmware anteriores a 1.0.4.30
- R6300v2, versiones de firmware anteriores a 1.0.4.32
- R6400, versiones de firmware anteriores a1.0.1.44
- R6400v2, versiones de firmware anteriores a 1.0.2.60
- R7000, versiones de firmware anteriores a 1.0.9.34
- R7100LG, versiones de firmware anteriores a 1.0.0.48
- R7300, versiones de firmware anteriores a 1.0.0.68
- R8000, versiones de firmware anteriores a 1.0.4.18
- R8000P, versiones de firmware anteriores a 1.4.1.24
- R7900P, versiones de firmware anteriores a 1.4.1.24
- R8500, versiones de firmware anteriores a 1.0.2.122
- R8300, versiones de firmware anteriores a 1.0.2.122
- WN2500RPv2, versiones de firmware anteriores a 1.0.1.54
- EX3700, versiones de firmware anteriores a 1.0.0.72
- EX3800, versiones de firmware anteriores a 1.0.0.72
- EX6000, versiones de firmware anteriores a 1.0.0.32
- EX6100, versiones de firmware anteriores a .1.0.2.24
- EX6120, versiones de firmware anteriores a 1.0.0.42
- EX6130, versiones de firmware anteriores a 1.0.0.24
- EX6150v1, versiones de firmware anteriores a 1.0.0.42
- EX6200, versiones de firmware anteriores a 1.0.3.88
- EX7000, versiones de firmware anteriores a 1.0.0.66
- D7000v2, versiones de firmware anteriores a 1.0.0.51

- D6220, versiones de firmware anteriores a 1.0.0.46
- D6400, versiones de firmware anteriores a 1.0.0.82
- D8500, versiones de firmware anteriores a 1.0.3.42
- WAC505, versiones de firmware anteriores a 5.0.0.17
- WAC510, versiones de firmware anteriores a 5.0.0.17
- WAC720, versiones de firmware anteriores a 5.0.0.17
- WAC730, versiones de firmware anteriores a 5.0.0.17
- WAC740, versiones de firmware anteriores a 5.0.0.17
- WND930, versiones de firmware anteriores a 5.0.0.17
- WC7500, versiones de firmware anteriores a 6.5.3.9
- WC7520, versiones de firmware anteriores a 6.5.3.9
- WC7600v1, versiones de firmware anteriores a 6.5.3.9
- WC7600v2, versiones de firmware anteriores a 6.5.3.9
- GS110EMX, versiones de firmware anteriores a 1.0.0.9
- GS810EMX, versiones de firmware anteriores a 1.0.0.5
- XS512EM, versiones de firmware anteriores a 1.0.0.6
- XS724EM, versiones de firmware anteriores a 1.0.0.6
- WAC505, versiones de firmware anteriores a 5.0.5.4
- WAC510, versiones de firmware anteriores a 5.0.5.4
- XR500, versiones de firmware anteriores a 2.3.2.32

Descripción:

Este aviso contiene 24 vulnerabilidades que afectan a productos de Netgear, 18 de las cuales son de severidad alta.

Solución:

Actualizar a la última versión de firmware disponible en el sitio: https://www.netgear.com/support/.

Detalle:

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

- Evadir la autenticación
- Acceder a información sensible
- Desbordar la pila (stack) tras la autenticación
- Desbordar la pila (stack) antes de la autenticación
- Instalar una versión de firmware anterior
- Inyectar comandos antes de la autenticación
- Inyectar comandos después de la autenticación
- Escalada vertical de privilegios
- Denegación de servicio
- Cross-site request forgery
- Realizar una configuración errónea de seguridad

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Vulnerabilidad de redirección abierta en WebSphere Portal de IBM

Fecha de publicación: 27/09/2018

Importancia: Alta

Recursos afectados:

- IBM WebSphere Portal desde la versión 9.0.0.0 hasta la versión 9.0.0.0 CF15
- IBM WebSphere Portal desde la versión 8.5.0.0 hasta la versión 8.5.0.0 CF15
- IBM WebSphere Portal desde la versión 8.0.0.0 hasta la versión 8.0.0.1 CF23
- IBM WebSphere Portal desde la versión 7.0.0.0 hasta la versión 7.0.0.2 CF30

Descripción:

IBM WebSphere Portal podría permitir a un atacante remoto realizar ataques de phishing, utilizando un ataque de redireccionamiento abierto.

Solución:

- Para las versiones 8.5 y 9.0 actualizar al CF16
- Para las versiones de la 8.0.0.0 hasta la 8.0.0.1 actualizar al Fix Pack 8.0.0.1 CF 23 y aplicar posteriormente el Interim Fix PH01459
- Para las versiones de la 7.0.0.0 hasta la 7.0.0.2 actualizar al Fix Pack 7.0.0.2 CF 30 y aplicar posteriormente el Interim Fix PH01459

Detalle:

- Al persuadir a una víctima para que visite un sitio web especialmente diseñado, un atacante remoto podría explotar esta vulnerabilidad para falsificar la URL mostrada y redirigir a un usuario a un sitio web malicioso. Esto podría permitir al atacante obtener información muy delicada o realizar nuevos ataques contra la víctima. Se ha reservado el identificador CVE-2018-1736 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Cisco IOS e IOS XE

Fecha de publicación: 27/09/2018

Importancia: Alta

Recursos afectados:

- Dispositivos que ejecutan versiones vulnerables de Cisco IOS e IOS XE Software, configuradas para operaciones OSPFv3.
- Software Cisco IOS XE en:
  - Cisco ASR 1000 Series Aggregation Services Routers:
    - ASR 1001-X
    - ASR 1001-HX
    - ASR 1002-X
    - ASR 1002-HX
    - Cisco ASR 1000 Series 100-Gbps Embedded Service Processor (ASR1000-ESP100)
    - Cisco ASR 1000 Series 200-Gbps Embedded Service Processor (ASR1000-ESP200)
  - Cisco 4000 Series Integrated Services Routers:
    - ISR 4431
    - ISR 4451-X
  - Si el software está configurado para terminar las conexiones IPsec VPN, incluyendo lo siguiente:
    - LAN-to-LAN VPN
    - Remote-access VPN, excluding SSL VPN
    - Dynamic Multipoint VPN (DMVPN)
    - FlexVPN
    - Group Encrypted Transport VPN (GET VPN)
    - IPsec virtual tunnel interfaces (VTIs)
    - Open Shortest Path First Version 3 (OSPFv3) con soporte para Autenticación con IPSec
- Software Cisco ASA y serie Cisco ASA 5500-X con software Firepower Threat Defense
  - Serie ASA 5506-X
  - Serie ASA 5508-X
  - Serie ASA 5516-X
- Swiches Cisco Catalyst series 3650 y 3850 versión 16.1.1
- Cisco IOS XE Software, con la cacterística servidor HTTP habilitada.
- Cisco ISR G2 o Cisco ISR4451-X Routers si tienen un módulo SM-X-1T3/E3 instalado y están ejecutando una versión afectada de Cisco IOS o IOS XE Software.
- Cisco IOS XE Software, configurado para NAT, y SIP ALG se activa cuando se configura el NAT en el dispositivo.
- Cisco Catalyst Switches que ejecuten una versión vulnerable de Cisco IOS Software o Cisco IOS XE Software con la función clúster habilitada y no fueran miembros del cúster desde la última recarga.
- Dispositivos que ejecuten Cisco IOS XE Software versión 16.6.1 o 16.6.2 con la función CDP activada en al menos una interfaz.
- Cisco Catalyst 3650, 3850 y 4500E que ejecuten una versión vulnerable de Cisco IOS XE con la función errdisable habilitada para una función, tanto a nivel de VLAN como de puerto.
- Cisco IOS XE Software.
- Cisco IOS Software o Cisco IOS XE Software configurados con IPv6.
- Cisco IOS Software configurado para procesar paquetes PTP (Precision Time Protocol):
  - 2500 Series Connected Grid Switches
  - Connected Grid Ethernet Switch Module Interface Card
  - Industrial Ethernet 2000 Series Switches
  - Industrial Ethernet 2000U Series Switches
  - Industrial Ethernet 3000 Series Switches
  - Industrial Ethernet 3010 Series Switches
  - Industrial Ethernet 4000 Series Switches
  - Industrial Ethernet 4010 Series Switches
  - Industrial Ethernet 5000 Series Switches

Descripción:

Cisco ha publicado 12 avisos de seguridad que describen 13 vulnerabilidades en Cisco IOS, todas ellas de criticidad alta.

Solución:

Cisco recomienda actualizar a las versiones más recientes de los productos afectados que se pueden encontrar en el siguiente enlace:

- Panel de descarga de Software Cisco

Detalle:

A continuación se detallan las 13 vulnerabilidades:

- Una vulnerabilidad en la implementación Open Shortest Path First versión 3 (OSPFv3), en Cisco IOS e IOS XE Software, podría permitir que un atacante cercano autenticado cause la recarga del dispositivo afectado, provocando una denegación de servicio (DoS). Esta vulnerabilidad está provocada por un manejo incorrecto de paquetes específicos de OSPFv3. Se ha reservado el identificador CVE-2018-0466 para esta vulnerabilidad.
- Una vulnerabilidad en el código del controlador IPSec de varias plataformas de software Cisco IOS XE y del dispositivo de seguridad adaptable (ASA) Cisco ASA serie 5500-X podría permitir que un atacante remoto no autenticado cause la recarga del dispositivo. La vulnerabilidad se debe a un procesamiento incorrecto del encabezado de autenticación IPSec mal formado (AH) o Encapsulating Security Payload (ESP). Se ha reservado el identificador CVE-2018-0472 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz de usuario web del software Cisco IOS XE podría permitir que un atacante remoto no autenticado, cause la recarga del dispositivo afectado, provocando una denegación de servicio (DoS). Esta vulnerabilidad se debe a un error double-free-in-memory por parte del software afectado cuando se procesan solicitudes HTTP específicas. Se ha reservado el identificador CVE-2018-0469 para esta vulnerabilidad.
- Una vulnerabilidad en el marco web del software Cisco IOS XE podría permitir que un atacante remoto no autenticado cause un desbordamiento del búfer en un dispositivo afectado, lo que da como resultado una condición de denegación de servicio (DoS). La vulnerabilidad se debe a que el software afectado analiza incorrectamente los paquetes HTTP mal formados destinados a un dispositivo. Se ha reservado el identificador CVE-2018-0470 para esta vulnerabilidad.
- Una vulnerabilidad en el firmware de los router SM-1T3/E3 de servicios integrados de segunda generación de Cisco (ISR G2) y del router de servicios integrados Cisco 4451-X (ISR4451-X), podría permitir que un atacante remoto no autenticado cause que se recarge el router ISR G2 o el Módulo SM-1T3/E3 del dispositivo ISR4451-X, lo que podría provocar una denegación de servicio (DoS). La vulnerabilidad se debe a un manejo inadecuado de la entrada del usuario. Se ha reservado el identificador CVE-2018-0485 para esta vulenrabilidad.
- Una vulnerabilidad en Network Address Translation (NAT) Session Initiation Protocol (SIP) Application Layer Gateway (ALG) del software Cisco IOS XE, podría permitir que un atacante remoto no autenticado provoque la recarga de un dispositivo afectado. Se ha reservado el identificador CVE-2018-0476 para esta vulenrabilidad.
- Una vulnerabilidad de validación de entrada incorrecta en el clúster de Cisco IOS Software y Cisco IOS XE Software podría permitir a un atacante no autenticado causar el bloqueo o sobrecarga del switch mediante el envío de un mensaje ICMP malicioso. Se ha reservado el identificador CVE-2018-0475 para esta vulnerabilidad.
- Un procesado incorrecto de ciertos paquetes CDP podría permitir a un atacante no autenticado provocar una fuga de memoria que

cause la denegación del servicio. Se ha reservado el identificador CVE-2018-0471 para esta vulnerabilidad.
- Una condición de carrera que ocurre cuando una VLAN y puerto entran en estado errsdisabled podría permitir a un atacante el bloqueo o sobrecarga del switch, provocando una denegación de servicio. Se ha reservado el identificador CVE- 2018-0480 para esta vulnerabilidad.
- Múltiples vulnerabilidades en el analizador CLI del software Cisco IOS XE Software, podrían permitir que un atacante local autenticado ejecute comandos en la shell Linux subyacente de un dispositivo afectado con privilegios de administrador. Se han reservado los identificadores CVE-2018-0477 y CVE-2018-0481 para estas vulnerabilidades.
- Una vulnerabilidad en el código de procesamiento de IPv6 de Cisco IOS Software y CiscoIOS XE Software podría permitir que un atacante remoto no autenticado, cause que el dispositivo se reinicie. Se ha reservado el identificador CVE-2018-0467 para esta vulnerabilidad.
- Una vulnerabilidad en el subsistema del Precision Time Protocol (PTP) del software Cisco IOS, podría permitir que un atacante remoto no autenticado, cause una condición de denegación de servicio (DoS) del PTP. Se ha reservado el identificador CVE-2018-0473 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

---

Vulnerabilidad XML Entity Expansion en IBM Platform Symphony e IBM Spectrum Symphony

Fecha de publicación: 28/09/2018

Importancia: Alta

Recursos afectados:

- IBM Platform Symphony 7.1 Fix Pack 1 y 7.1.1
- IBM Spectrum Symphony 7.1.2 y 7.2.0.2

Descripción:

Una vulnerabilidad de XML Entity Expansion (XXE) afecta a los productos IBM Platform Symphony e IBM Spectrum Symphony.

Solución:

Los parches de seguridad pueden ser descargados desde IBM Fix Central:

- sym-7.1-build494537
- sym-7.1.1-build494444
- sym-7.1.2-build494315
- sym-7.2.0.2-build494326

Detalle:

IBM Spectrum Symphony es vulnerable a un ataque XML External Entity Injection (XXE) al procesar datos XML. Un atacante remoto podría aprovechar esta vulnerabilidad para exponer información confidencial o consumir recursos de memoria. Se ha reservado el identificador CVE-2018-1702 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad