Boletín de mayo de 2019

Avisos Técnicos

Vulnerabilidad en SD-WAN Appliance de Citrix

Fecha de publicación: 02/05/2019

Importancia: Alta

Recursos afectados:

- Todas las versiones de:
  - NetScaler SD-WAN 9.x
  - NetScaler SD-WAN 10.0.x anteriores a 10.0.7
  - Citrix SD-WAN 10.1.x
  - Citrix SD-WAN 10.2.x anteriores a 10.2.2

Descripción:

Los investigadores Sergey Gordeychik, Denis Kolegov y Nikita Oleksov del equipo SD-WAN New Hop(e), trabajando conjuntamente con Citrix, han identificado una vulnerabilidad de criticidad alta que podría permitir a un atacante realizar un ataque del tipo *man-in-the-middle*.

Solución:

Citrix ha publicado actualizaciones que mitigan la vulnerabilidad en función del producto y versión afectada:

- Actualizar NetScaler SD-WAN a la versión 10.0.7
- Actualizar Citrix SD-WAN a la versión 10.2.2

Los usuarios registrados pueden acceder a las actualizaciones a través del centro de descargas de Citrix

Detalle:

- La vulnerabilidad de divulgación de información en Citrix SD-WAN Appliance, podría permitir a un atacante, sin autenticar, realizar un ataque *man-in-the-middle* contra el gestor de tráfico. Se ha reservado el identificador CVE-2019-11550 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de denegación de servicio en productos de F5

Fecha de publicación: 02/05/2019

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) versiones:
  - desde la 14.0.0 hasta la 14.1.0
  - desde la 13.0.0 hasta la 13.1.1
  - desde la 12.1.0 hasta la 12.1.4
  - desde la 11.6.1 hasta la 11.6.3
  - desde la 11.5.1 hasta la 11.5.8

Descripción:

F5 ha publicado dos vulnerabilidades de severidad alta, que afectan a varios de sus productos. La explotación exitosa de alguna de estas

vulnerabilidades podría provocar una condición de denegación de servicio (DoS) al provocar que el TMM (*Trafic Management Microkernel*) se reinicie.

Solución:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) versiones:
  - desde la 14.0.0 hasta la 14.1.0 actualizar a la 14.1.0.2
  - desde la 13.0.0 hasta la 13.1.1 actualizar a la 13.1.1.5
  - desde la 12.1.0 hasta la 12.1.4 actualizar a la 12.1.4.1
  - desde la 11.6.1 hasta la 11.6.3 actualizar a la 11.6.4
  - desde la 11.5.1 hasta la 11.5.8 actualizar a la 11.5.9

Detalle:

- Una de las dos vulnerabilidades afecta al servidor virtual BIG-IP si tiene un perfil TCP y DNS y si además tiene habilitada la memoria caché de DNS, en caso de que las conexiones TCP de consultas DNS se cancelen antes de recibir una respuesta del caché de DNS, se podría originar una condición de denegación de servicio (DoS), al provocar un reinicio del TMM. Se ha reservado el identificador CVE-2019-6612 para esta vulnerabilidad.
- La otra vulnerabilidad, que se da al procesar ciertas secuencias raras de datos que tienen lugar en el tráfico VPN PPTP, podría causar que el TMM se reinicie, lo que daría lugar a una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-6611 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 02/05/2019

Importancia: Crítica

Recursos afectados:

- Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI).
- Cisco AsyncOS Software para Cisco Web Security Appliance, tanto en dispositivos virtuales como en dispositivos hardware.
- Cisco Umbrella Dashboard.
- 3000 Series Industrial Security Appliances (ISAs).
- Adaptive Security Appliance (ASA):
  - 1000V Cloud Firewall.
  - 5505 Series Adaptive Security Appliance (ASA 5500 Series Adaptive Security Appliances distintos a ASA 5505 han alcanzado el hito de fin de soporte y ya no se evalúan en cuanto a vulnerabilidades de seguridad).
  - 5500-X Series Firewalls.
  - Services Module para Cisco Catalyst 6500 Series Switches y Cisco 7600 Series Routers.
  - 5500-X Series con FirePOWER Services.
- Adaptive Security Virtual Appliance (ASAv).
- Firepower:
  - 2100 Series.
  - 4100 Series.
  - 9300 ASA Security Module.
  - Threat Defense Virtual.
  - 7000 Series Appliances.
  - 8000 Series Appliances.
  - 9300 Security Appliances.
- Versiones anteriores a 1.4.10.6 de los productos:
  - Small Business 200 Series Smart Switches.
  - Small Business 300 Series Managed Switches.
  - Small Business 500 Series Managed Switches.
- Versiones anteriores a 2.5.0.78 de los productos:
  - 250 Series Smart Switches.
  - 350 Series Managed Switches.
  - 350X Series Managed Switches.
  - 550X Series Stackable Managed Switches.
- Cisco Small Business RV320 y RV325 Dual Gigabit WAN VPN Routers, versiones de *firmware* anteriores a 1.4.2.20
- IP Conference Phone 7832 y 8832
- IP Phone 7811, 7821, 7841, 7861, 8811, 8841, 8845, 8851, 8861 y 8865
- Unified IP 8831 Conference Phone (su solución está prevista para finales de 2019) y Unified IP 8831 Conference Phone para Third-Party Call Control (aún sin solución).
- Wireless IP Phone 8821 y 8821-EX.
- Advanced Malware Protection (AMP) para Networks en:
  - FirePOWER 7000 Series Appliances.
  - FirePOWER 8000 Series Appliances.
  - FirePOWER 9300 Series Appliances.
- Firepower Threat Defense para Integrated Services Routers (ISRs).
- FTD Virtual (FTDv).
- Next-Generation Intrusion Prevention System (NGIPS).
- Productos de Cisco que ejecutan una versión vulnerable de Cisco ASA Software y tienen habilitado el acceso a la gestión web.
- Cisco Application Policy Infrastructure Controller (APIC) Software, versiones anteriores a 4.1(1i).
- Cisco Nexus 9000 Series ACI Mode Switch Software, versiones anteriores a 14.1(1i).

Descripción:

Cisco ha publicado 22 vulnerabilidades, siendo una de ellas de severidad crítica y el resto de severidad alta.

Solución:

- Cisco ha publicado actualizaciones, en función del producto afectado, que solucionan las vulnerabilidades. Puede acceder a las actualizaciones desde el panel de descargas de software de Cisco.

Detalle:

Los tipos de vulnerabilidades son las siguientes, con sus correspondientes identificadores, todos ellos reservados:

- Fallo en la gestión de claves SSH: CVE-2019-1804.
- Escalada de privilegios: CVE-2019-1816, CVE-2019-1803, CVE-2019-1682 y CVE-2019-1592.
- Denegación de servicio: CVE-2019-1817, CVE-2018-15388, CVE-2019-1635, CVE-2019-1696, CVE-2019-1704, CVE-2019-1703, CVE-2018-15462, CVE-2019-1706, CVE-2019-1708, CVE-2019-1693 y CVE-2019-1694.
- Fallo en la funcionalidad de gestión de sesiones: CVE-2019-1807.
- Omisión de autenticación: CVE-2019-1859 y CVE-2019-1714.
- Secuestro de sesión: CVE-2019-1724.
- Insuficiente entropía en la generación de claves criptográficas: CVE-2019-1715.
- *Cross-Site Request Forgery* (CSRF): CVE-2019-1713.
- Autenticación de cliente TLS insegura: CVE-2019-1590.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos SAP

Fecha de publicación: 03/05/2019

Importancia: Crítica

Recursos afectados:

- SAP S/4HANA®
- SAP Enterprise Resource Planning (ERP)
- SAP Product Lifecycle Management (PLM)
- AP Customer Relationship Management (CRM)
- SAP Human Capital Management (HCM)
- SAP Supply Chain Management (SCM)
- SAP Supplier Relationship Management (SRM)
- SAP NetWeaver® Business Warehouse (BW)
- SAP Business Intelligence (BI)
- SAP Process Integration (PI)
- SAP Governance
- SAP Solution Manager (SolMan)
- Risk & Compliance 10.x (GRC)
- SAP NetWeaver ABAP® Application Server 7.0 - 7.52

Descripción:

Durante la OPCDE Security Conference celebrada en Dubai, en abril de 2019, se han hecho públicas varias vulnerabilidades asociadas a errores de configuración y de severidad crítica denominadas *10KBLAZE*. Estas vulnerabilidades podrían comprometer a diversas aplicaciones SAP incluyendo la eliminación de todos los datos de aplicación de negocio, modificación o extracción de información sensible.

Las vulnerabilidades ya fueron detectadas y parcheadas por SAP en 2005, 2009 y 2019; pero debido al conocimiento de estos errores de configuración, a la posibilidad de su explotación activa, y a su criticidad se recomienda seguir las recomendaciones de SAP a la hora de realizar las instalaciones y configuraciones de los sistemas.

Solución:

- Aplique las notas de seguridad de SAP: #821875 (2005), #1408081 (2009) y #1421005 (2010). Los clientes de SAP pueden acceder al contenido de las notas a través del portal de soporte de SAP (se necesita autenticación).
- Implementar las funciones de detección en cortafuegos y dispositivos IPS/IDS con las reglas de firma de Snort. Se han hecho públicas las firmas a proveedores de cortafuegos reconocidos como Cisco, FireEye y Palo Alto.

Detalle:

- Las vulnerabilidades expuestas son debidas a fallos de configuración administrativa en instalaciones SAP Netweaver, si estas no se han realizado con las recomendaciones proporcionadas por SAP.
- Se recomienda tomar medidas con la mayor urgencia posible, ya que estos fallos de configuración son conocidos públicamente y podrían estar siendo empleados activamente.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad XXE en IBM TRIRIGA

Fecha de publicación: 06/05/2019

Importancia: Alta

Recursos afectados:

- IBM TRIRIGA Application Platform, versión 3.5.3 y 3.6.0

Descripción:

Existe una vulnerabilidad de inyección XXE (*XML External Entity*) en IBM TRIRIGA Application Platform.

Solución:

- Aplicar los parches de IBM TRIRIGA Application Platform, versión 3.5.3.6 y 3.6.0.3.

Detalle:

- IBM TRIRIGA es vulnerable a un ataque XXE (*XML External Entity*) 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-2019-4208 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Print Management Software de PrinterLogic

Fecha de publicación: 06/05/2019

Importancia: Alta

Recursos afectados:

- PrinterLogic versión 18.3.1.96 y anteriores

Descripción:

El software PrinterLogic Print Management no valida los certificados SSL ni de actualización de software, lo que podría permitir a un atacante reconfigurar el software y ejecutar el código de forma remota. Además, el agente PrinterLogic no valida la entrada del navegador, lo que podría permitir a un atacante remoto modificar la configuración. Estas vulnerabilidades pueden dar lugar a la ejecución de código remoto en estaciones de trabajo que ejecuten el agente PrinterLogic.

Solución:

- Actualizar PrinterLogic cuando los parches estén disponibles.
- Considerar utilizar VPN para evitar escenarios MITM y aplicar listas blancas de aplicaciones para evitar que el agente PrinterLogic ejecute código malicioso.

Detalle:

- El software PrinterLogic Print Management no valida, o valida incorrectamente, el certificado SSL del portal de gestión PrinterLogic. Cuando un certificado es inválido o malicioso, puede permitir que un atacante suplante a una entidad de confianza utilizando un ataque *Man In The Middle* (MITM). El software puede conectarse a un host malicioso creyendo que que es un host de confianza, o puede ser engañado para que acepte datos que parecen provenir de un host de confianza. Se ha reservado el identificador CVE-2018-5408 para esta vulnerabilidad.
- El software PrinterLogic Print Management actualiza y ejecuta código sin verificar, suficientemente, su origen e integridad. Un atacante puede ejecutar código malicioso comprometiendo el servidor host, realizando *spoofing* DNS o modificando el código en tránsito. Se ha reservado el identificador CVE-2018-5409 para esta vulnerabilidad.
- El software PrinterLogic Print Management no desinfecta los caracteres especiales, lo que permite realizar cambios remotos no autorizados en los archivos de configuración. Se ha reservado el identificador CVE-2019-9505 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en IBM InfoSphere Information Server

Fecha de publicación: 07/05/2019

Importancia: Alta

Recursos afectados:

- IBM InfoSphere Information Server, versión 11.7.1
- IBM InfoSphere Information Server en Cloud, versión 11.7.1

Descripción:

En IBM InfoSphere Information Server se ha detectado una vulnerabilidad de escalada de privilegios.

Solución:

- IBM no ha publicado una solución para esta vulnerabilidad. Sin embargo, se pueden seguir los pasos descritos en la sección *Workarounds and Mitigations* del aviso del fabricante para securizar el entorno de trabajo.

Detalle:

- Los contenedores de IBM InfoSphere Information Server son vulnerables a una escalada de privilegios debido a un componente configurado de forma insegura. Se ha reservado el identificador CVE-2019-4185 para esta vulnerabilidad.

Etiquetas: 0day, IBM, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.6

Fecha de publicación: 08/05/2019

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones desde 1.7.0 hasta 3.9.5.

Descripción:

Joomla! ha publicado una nueva versión que soluciona una vulnerabilidad de criticidad baja en su núcleo. Esta vulnerabilidad es de tipo

cross-site scripting (XSS).

Solución:

- Actualizar a la versión 3.9.6.

Detalle:

- Las vistas de depuración de *com_users* no saneaban correctamente los datos suministrados por el usuario, lo que permite realizar un ataque XSS. Se ha reservado el identificador CVE-2019-11809 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de salto de autenticación en Cisco Elastic Services Controller

Fecha de publicación: 08/05/2019

Importancia: Crítica

Recursos afectados:

- Cisco Elastic Services Controller, ejecutando versiones de sofware 4.1, 4.2, 4.3, o 4.4 con REST API habilitado.

Descripción:

Se ha detectado una vulnerabilidad de severidad crítica en Cisco Elastic Services Controller (ESC) que podría permitir a un atacante remoto sin autenticación saltarse la autenticación en REST API y realizar acciones en el sistema.

Solución:

- Cisco ha publicado una actualización que mitiga la vulnerabilidad en función de la versión de software. Es posible descargarla desde su centro de descarga de software.
- Las versiones afectadas:
  - 4.1 actualizar a las versiones:
    - 4.1.0.100
    - 4.1.0.111
  - 4.2 actualizar a las versiones:
    - 4.2.0.74
    - 4.2.0.86
  - 4.3 actualizar a las versiones:
    - 4.3.0.121
    - 4.3.0.128
    - 4.3.0.134
    - 4.3.0.135
  - 4.4 actualizar a las versiones:
    - 4.4.0.80
    - 4.4.0.82
    - 4.4.0.86
- La versión 4.5 y las anteriores a la 4.1 no se encuentran afectadas.

Detalle:

- La vulnerabilidad se debe a una validación incorrecta en las peticiones a la API. Un atacante podría explotar esta vulnerabilidad enviando una petición especialmente generada a la REST API, lo que podría permitir al atacante ejecutar acciones a través de la REST API con privilegios de administrador en el sistema afectado. Se ha reservado el identificador CVE-2019-1867 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Intelligent Management Center de HPE

Fecha de publicación: 10/05/2019

Importancia: Crítica

Recursos afectados:

- Intelligent Management Center.

Descripción:

Matthias Kaiser y Steven Seeley, de Incite Team, han publicado un total de 8 vulnerabilidades, siendo una de ellas de severidad media, 5 altas y 2 críticas. Las vulnerabilidades descritas podrían permitir ataques de ejecución remota de código y de divulgación de credenciales criptográficas.

Solución:

- Aún no existe actualización que corrija estas vulnerabilidades. Como medida de mitigación, se recomienda restringir la interacción con el servicio a máquinas de confianza. Solo los clientes y servidores que tengan una relación procesal legítima con el servicio deben poder comunicarse con él. Esto podría lograrse de varias maneras, sobre todo con reglas en el *firewall* o listas blancas.

Detalle:

Las vulnerabilidades de severidad crítica son:

- Existe un fallo específico en el *endpoint AccessMgrServlet*. Al analizar las solicitudes, el proceso no valida correctamente los datos suministrados por el usuario, lo que puede dar lugar a la deserialización de los datos no fiables. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.
- Se produce un error en el manejo de las peticiones AMF3 hasta el *endpoint amf*. El problema se debe a la falta de validación adecuada de los datos suministrados por el usuario, que puede dar lugar a la deserialización de los datos no confiables. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.

Etiquetas: 0day, HP, Vulnerabilidad

XML External Entity en IBM i2 Intelligence Analysis Platform

Fecha de publicación: 10/05/2019

Importancia: Alta

Recursos afectados:

- IBM i2 Analyst's Notebook 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.1.0 y 9.1.1
- IBM i2 Analyst's Notebook Premium 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.0.8, 9.1.0 y 9.1.1
- IBM i2 Enterprise Insight Analysis

Descripción:

IBM i2 Intelligent Analyis Platform ha solucionado una vulnerabilidad de XXE (*XML External Entity)* que podría permitir a los atacantes obtener acceso a información confidencial o hacer que el sistema del usuario realice llamadas a servidores remotos.

Solución:

- IBM i2 Analyst's Notebook Version 9.0.6
- IBM i2 Analyst's Notebook Version 9.1.1
- IBM i2 Analyst's Notebook Premium Version 9.06
- IBM i2 Analyst's Notebook Premium Version 9.1.1

No existe parche para el resto de versiones afectadas, se recomienda actualizar a las versiones anteriores.

Detalle:

- IBM i2 Intelligent Analyis Platform es vulnerable a un ataque de inyección de entidad externa XML (XXE) 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-2019-4062 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en SQLite

Fecha de publicación: 10/05/2019

Importancia: Alta

Recursos afectados:

- SQLite, versiones 3.26.0 y 3.27.0

Descripción:

El investigador Cory Duplantis, de Cisco Talos, ha descubierto que SQLite contiene una vulnerabilidad explotable de tipo uso posterior a liberación de memoria que podría permitir a un atacante obtener la capacidad de ejecutar código de forma remota en el equipo objetivo.

Solución:

- SQLite, en colaboración con Cisco Talos, ha publicado una actualización para los clientes afectados, que se puede obtener desde su página de descargas.

Detalle:

- SQLite implementa la característica *Window Functions* de SQL, que permite realizar consultas sobre un subconjunto, o *window*, de filas. Esta vulnerabilidad específica reside en la función *window*. Un comando SQL, especialmente diseñado, podría causar una vulnerabilidad de uso posterior a liberación de memoria, lo que puede resultar en la ejecución remota de código. Se ha reservado el identificador CVE-2019-5018 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Cross-Site Scripting (XSS) persistente en Liferay

Fecha de publicación: 13/05/2019

Importancia: Alta

Recursos afectados:

- com.liferay.faces.alloy-2.0.0 (Liferay Portal 6.2)
- com.liferay.faces.alloy-2.0.1 (Liferay Portal 6.2)
- com.liferay.faces.alloy-3.0.0 (Liferay Portal 7.0)
- com.liferay.faces.alloy-3.0.1 (Liferay Portal 7.0)
- liferay-faces-alloy-3.2.5-ga6 (Liferay Portal 6.2)
- liferay-faces-alloy-4.2.5-ga6 (Liferay Portal 6.2)

Descripción:

Se ha publicado una vulnerabilidad Cross-Site Scripting (XSS) persistente en algunas versiones Liferay Faces Alloy.

Solución:

- Aplicar el parche adecuado en función de la versión afectada.

Detalle:

- Existe una vulnerabilidad Cross-Site Scripting (XSS) persistente en *alloy:autoComplete* y *alloy:inputFile* debido a una representación incorrecta de las cadenas JavaScript en los arrays de las versiones de Liferay Faces Alloy afectadas.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en la funcionalidad pingback de los blogs de Liferay

Fecha de publicación: 14/05/2019

Importancia: Crítica

Recursos afectados:

- Liferay Portal 7.0 CE GA7 (7.0.6) y versiones anteriores sin soporte.

Descripción:

El investigador Christian Mehlmauer ha reportado una vulnerabilidad que afecta a la funcionalidad *pingback* en los blogs que podría utilizarse para realizar ataques de escaneo de puertos.

Solución:

- No existe parche para esta vulnerabilidad. Como medida de mitigación, se recomienda desactivar la funcionalidad *pingback*. Se recomienda actualizar el portal a Liferay Portal 7.1 CE GA1 (7.1.0) o posterior.

Detalle:

- Esta vulnerabilidad permite a atacantes remotos enviar solicitudes HTTP a servidores de Internet y realizar ataques de escaneo de puertos, especificando una URL de origen falsa.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en múltiples productos de Citrix

Fecha de publicación: 14/05/2019

Importancia: Crítica

Recursos afectados:

- Receiver para Windows, versiones anteriores a LTSR 4.9 CU6 4.9.6001
- Citrix Workspace App, versiones anteriores a 1904

Descripción:

Los investigadores Ollie Whitehouse, Richard Warren y Martin Hill, de NCC Group, han descubierto una vulnerabilidad de ejecución remota de código en los productos Citrix Workspace App y Receiver para Windows.

Solución:

- Citrix recomienda que los clientes actualicen a la versión 1904 o posterior de Citrix Workspace App, y a la versión LTSR 4.9 CU6 4.9.6001 de Receiver para Windows.

Detalle:

- Se ha identificado una vulnerabilidad en los productos Citrix Workspace App y Receiver para Windows, que podría provocar que no se apliquen las preferencias de acceso a la unidad local, lo que permitiría a un atacante leer/escribir el acceso a las unidades locales de los clientes, otorgando la posibilidad de realizar una ejecución remota de código en el dispositivo del cliente. Se ha reservado el identificador CVE-2019-11634 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 14/05/2019

Importancia: Alta

Recursos afectados:

- Dispositivos Cisco que utilicen una versión afectada del software Cisco IOS XE con la función de servidor HTTP activada. El estado predeterminado de la función Servidor HTTP depende de la versión.
- La vulnerabilidad de modificación de hardware Cisco Secure Boot afecta a varios productos de Cisco que admiten la funcionalidad de arranque seguro basado en hardware, para ver el listado completo consulte la tabla de productos afectados en la sección de *Referencias*.

Descripción:

Cisco ha publicado dos vulnerabilidades, una en la interfaz de usuario basada en web (Web UI) de Cisco IOS XE Software que podría permitir a un atacante remoto autenticado ejecutar comandos en el shell Linux subyacente de un dispositivo afectado con privilegios de root, y otra en Secure Boot de Cisco, que podría permitir escribir una imagen de *firmware* modificada en el componente.

Solución:

- Cisco ha publicado actualizaciones de software gratuitas que abordan las vulnerabilidades descritas en este aviso.

Detalle:

- El software afectado sanea incorrectamente la entrada suministrada por el usuario en la interfaz de usuario basada en web (Web UI) de Cisco IOS XE Software. Un atacante que tenga acceso de administrador a un dispositivo afectado podría explotar esta vulnerabilidad suministrando un parámetro de entrada, especialmente diseñado, en un formulario, en la interfaz de usuario de la Web y enviándolo posteriormente. Esto podría permitir al atacante ejecutar comandos arbitrarios en el dispositivo con privilegios de root, lo que puede llevar a un compromiso completo del sistema. Se ha asignado el identificador CVE-2019-1862 para esta vulnerabilidad.
- Una comprobación incorrecta en el área de código que gestiona las actualizaciones *in situ* de una parte de la implementación de hardware de arranque seguro de *Field Programmable Gate Array (FPGA)*, podría permitir que un atacante con privilegios elevados y acceso al sistema operativo subyacente que se está ejecutando en el dispositivo afectado, escribiera una imagen de firmware modificada en la FPGA, causando que el dispositivo se vuelva inutilizable (y requerir un reemplazo de hardware) o manipulando el proceso de verificación de arranque seguro, lo que en algunas circunstancias puede permitir al atacante instalar y arrancar una imagen de software malicioso. Se ha asignado el identificador CVE-2019-1649 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de man-in-the-middle en Samba

Fecha de publicación: 14/05/2019

Importancia: Alta

Recursos afectados:

- Todas las versiones desde Samba 4.0.
- Todas las versiones de Heimdal, desde 0.8 incluyendo 7.5.0, y cualquier producto que envíe un KDC (*Key Distribution Center*) derivado de una de esas versiones de Heimdal.

Descripción:

La validación del *checksum* en el *handler* S4U2Self, en el KDC Heimdal integrado, no confirmó inicialmente que el *checksum* estuviera descifrado, permitiendo la sustitución del principal objetivo (cliente) solicitado.

Solución:

- Se han publicado parches que abordan esta vulnerabilidad en el centro de descargas de Samba. Adicionalmente, se han publicado las versiones de Samba 4.8.12, 4.9.8 y 4.10.3 como parches de seguridad para corregir el fallo. Se aconseja a los administradores de Samba que actualicen a estas versiones o que apliquen el parche lo antes posible.

Detalle:

- Hay un defecto en el Active Directory (AD) Domain Controller (DC) de Samba en el KDC de Heimdal. Cuando Heimdal KDC comprueba el *checksum* que el servidor coloca en el paquete S4U2Self para proteger la entidad de seguridad solicitada contra modificaciones, no confirma que el algoritmo de *checksum* que protege el nombre de usuario en la solicitud esté cifrado. Esta situación permite realizar un ataque de tipo *man-in-the-middle* que puede interceptar la solicitud y modificarla mediante el reemplazo del nombre de usuario de la solicitud por otro nombre de usuario cualquiera que se encuentre en el KDC. Se ha reservado el identificador CVE-2018-16860 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Samba, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de HP

Fecha de publicación: 15/05/2019

Importancia: Alta

Recursos afectados:

- Servidores HPE ProLiant Gen10, con versiones *firmware* de SPS (*Server Platform Services*) anteriores a 4.00.04.393, modelos:
  - DL360
  - DL120

    - DL160
    - DL180
    - DL580
    - DL380
    - DL560
- Servidores HPE ProLiant Gen10, con versiones *firmware* de SPS anteriores a 5.00.04.024, modelos:
    - ML110
    - ML350
    - XL170r
    - XL190r
    - XL230k
    - XL270d
    - XL450
    - DL20
    - ML30
- Servidores HPE ProLiant Gen9, con versiones firmware de SPS anteriores a 4.01.04.054, modelos:
    - ML30
    - DL20

Descripción:

El equipo de respuesta de seguridad de productos HPE ha descubierto varias vulnerabilidades en múltiples productos de HP.

Solución:

- HPE ha proporcionado *firmware* actualizado para hacer frente a estas vulnerabilidades que se puede descargar desde el centro de soporte de HPE.

Detalle:

- Diversas vulnerabilidades de seguridad en Intel® CSME, Server Platform Services, Trusted Execution Engine e Intel® Active Management Technology pueden permitir a los usuarios realizar una escalada de privilegios, divulgar información o provocar una denegación de servicio, lo que impactaría en varios productos de HP. Se han reservado los identificadores CVE-2019-0089 y CVE-2019-0090 para estas vulnerabilidades.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 15/05/2019

Importancia: Alta

Recursos afectados:

Productos afectados por vulnerabilidades de severidad alta:

- Intel® NUC Kit NUC8i7HNK, BIOS version 0054 o posterior.
- Intel® NUC Kit NUC8i7HVK, BIOS version 0054 o posterior.
- Intel® NUC Kit NUC7i7DNHE, BIOS version 0062 o posterior.
- Intel® NUC Kit NUC7i7DNKE, BIOS version 0062 o posterior.
- Intel® NUC Kit NUC7i5DNHE, BIOS version 0062 o posterior.
- Intel® NUC Kit NUC7i5DNHE, BIOS version 0062 o posterior.
- Intel® NUC Board NUC7i7DNBE, BIOS version 0062 o posterior.
- Intel® CSME, versiones anteriores a 11.8.65, 11.11.65, 11.22.65 y 12.0.35.
- Intel® Server Platform Services, versiones anteriores a SPS_E3_05.00.04.027.0.
- Intel® Trusted Execution Engine, anterior a TXE 3.1.65, 4.0.15.
- Intel® Xeon® Processor D Family.
- Intel® Xeon® Scalable Processor.
- Intel® Server Board.
- Intel® Server System.
- Intel® Compute Module.
- Intel® Pentium® Processor J Series.
- Intel® Pentium® Processor N Series.
- Intel® Celeron® J Series.
- Intel® Celeron® N Series.
- Intel® Atom® Processor A Series.
- Intel® Atom® Processor E3900 Series.
- Intel® Pentium® Processor Silver Series.
- Intel® i915 Graphics for Linux, versión anterior a la 5.0

Productos afectados por vulnerabilidades de severidad media:

- Intel® PROSet/Wireless WiFi Software, versión 20.100 y anteriores.
- 4th Generation Intel® Core™/ Pentium®/ Xeon® (E3 v3 only) Processor (Haswell) systems, ejecutando Windows® 7 o Windows® 8.1 con Intel® Graphics Driver para Windows, versión anterior a 10.18.14.5067 (también conocida como 15.36.x.5067) y 10.18.10.5069 (también conocida como 15.33.x.5069).
- 3rd Generation Intel® Core ™/ Pentium®/ Celeron®/ Xeon® (E3 v2 only) Processor (Ivybridge) systems con Intel® Graphics Driver para Windows, versión anterior a 10.18.14.5067 (también conocida como 15.36.x.5067) y 10.18.10.5069 (también conocida como 15.33.x.5069).
- Intel® Pentium®/ Celeron®/ Atom® Processor (Baytrail) systems con Intel® Graphics Driver para Windows, versión anterior a 10.18.14.5067 (también conocida como 15.36.x.5067) y 10.18.10.5069 (también conocido como 15.33.x.5069).
- Intel Unite® Client versión anterior a la 3.3.176.13.
- Los productos listados en el siguiente enlace.
- Intel® SCS Discovery Utility: SCS_download_package before, versión 12.0.0.129.
- Intel® ACU Wizard: Configurator_download_package before, versión 12.0.0.129.
- Intel® Quartus® Prime, todas las versiones desde la 15.1 hasta la 18.1.
- Intel® Quartus® II, versiones desde la 9.1 hasta la 15.0.
- Intel Unite® Client for Android, versión anterior a la 4.0.
- Intel® Driver & Support Assistant, versión 19.3.12.3 y anteriores.

Descripción:

Intel ha publicado 12 avisos de seguridad en su centro de seguridad de productos, 4 de severidad alta y 8 de severidad media.

Solución:

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

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

Se han asignado los siguientes identificadores: CVE-2019-11094, CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, CVE-2019-0099, CVE-2019-0153, CVE-2019-0170, CVE-2019-0119, CVE-2019-0120, CVE-2019-0126, CVE-2019-11085, CVE-2018-3701, CVE-2019-0113, CVE-2019-0114, CVE-2019-0115, CVE-2019-0116, CVE-2019-0132, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-0138, CVE-2019-11093, CVE-2019-0171, CVE-2019-0172, CVE-2019-11114 y CVE-2019-11095.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en TIBCO Spotfire

Fecha de publicación: 15/05/2019

Importancia: Crítica

Recursos afectados:

Está afectado la interfaz web de los siguientes productos:

- TIBCO Spotfire Statistics Services, versiones 7.11.1 y anteriores.
- TIBCO Spotfire Statistics Services, versión 10.0.0

Está afectado el servidor web de los siguientes productos:

- TIBCO Spotfire Analytics Platform para AWS Marketplace, versiones 7.14.0, 7.14.1, 10.0.0, 10.0.1, 10.1.0 y 10.2.0
- TIBCO Spotfire Server, versiones 7.14.0, 10.0.0, 10.0.1, 10.1.0 y 10.2.0

Descripción:

TIBCO ha reportado dos vulnerabilidades en sus productos TIBCO Spotfire, una de ellas afecta a la interfaz web y expone ficheros sensibles, y la otra es del tipo *Cross-Site Scripting* (XSS) reflejado y afecta al servidor web.

Solución:

TIBCO ha lanzado versiones actualizadas de los componentes afectados que abordan estos problemas:

- Las versiones 7.11.1 y posteriores de TIBCO Spotfire Services Services se actualizan a la versión 7.11.2 o superior.
- La versión 10.0.0 de TIBCO Spotfire Statistics Services se actualiza a 10.0.1 o superior.
- La plataforma TIBCO Spotfire Analytics para AWS Marketplace, versiones 7.14.0, 7.14.1, 10.0.0, 10.0.1, 10.1.0 y 10.2.0, se actualiza a 10.3.0 o superior.
- Las versiones 7.1.4.0, 10.0.0, 10.0.1, 10.1.0 y 10.2.0 del servidor TIBCO Spotfire se actualizan a 10.2.1 o superior.

Detalle:

- La vulnerabilidad que expone archivos confidenciales afecta a la interfaz web y podría permitir que un usuario autenticado acceda a información confidencial del servidor de servicios de estadísticas de Spotfire. La información confidencial que podría verse afectada incluye bases de datos, JMX, LDAP, cuentas de servicio de Windows y credenciales de usuario. Se ha asignado el identificador CVE-2019-11204 a esta vulnerabilidad.
- La vulnerabilidad del tipo *Cross-Site Scripting* (XSS) reflejado afecta al servidor web y podría permitir que un atacante no autenticado ganara acceso administrativo a la interfaz web del servidor web. Se ha asignado el identificador CVE-2019-11205 a esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de mayo de 2019

Fecha de publicación: 15/05/2019

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player.
- Microsoft Windows.
- Internet Explorer.
- Microsoft Edge.
- Microsoft Office y Microsoft Office Services y Web Apps.
- Team Foundation Server.
- Visual Studio.
- Azure DevOps Server.

- SQL Server.
- .NET Framework.
- .NET Core.
- ASP.NET Core.
- ChakraCore.
- Online Services.
- Azure.
- NuGet.
- Skype para Android.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft de este mes consta de 78 vulnerabilidades, 22 clasificadas como críticas y 56 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:

- Escalada de privilegios.
- Ejecución remota de código.
- Denegación de servicio.
- Omisión de característica de seguridad.
- Divulgación de información.
- Suplantación.
- Falsificación.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Actualización de seguridad de SAP de mayo de 2019

Fecha de publicación: 15/05/2019

Importancia: Alta

Recursos afectados:

- SAP Identity Management (REST Interface), versión 2
- SAP BusinessObjects Business Intelligence platform (Central Management Server), versiones 4.20, 4.30
- SAP Treasury and Risk Management, versiones 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 617, 6.18, 8.0
- SAP E-Commerce (Business-to-Consumer), versiones (SAP-CRMJAV SAP-CRMWEB SAP-SHRWEB SAP-SHRJAV SAP-CRMAPP SAP-SHRAPP) 7.30, 7.31, 7.32, 7.33, 7.54
- SAP BusinessObjects Business Intelligence platform, versiones 4.2, 4.3
- Web Dynpro Java, versiones - 6.40, 7.00, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP Solution Manager system (ST-PI), versiones 2008_1_700, 2008_1_710 y 740
- Software Component - KRNL32NUC, versiones 7.20 y 7.20EXT
- Software Component - KRNL32UC, versiones 7.20 y 7.20EXT
- Software Component - KRNL64NUC, versiones 7.20 y 7.20EXT
- Software Component - KRNL64UC, versiones 7.20, 7.2L, 7.20EXT y 8.00
- Software Component - KERNEL, versiones 7.20, 7.2L y 8.00
- Software Component - SAP BASIS, versiones 46D, 6.40, desde 7.00 hasta 7.02, 7.10, 7.30, 7.31 y 7.40
- Dbpool of AS JAVA, versiones 6.40, 7.00, 7.01, 7.10, 7.11, 7.20, 7.30, 7.31 y 7.40
- Dbpool of AS JAVA, versiones 6.40, 7.00, 7.01, 7.10, 7.11, 7.20, 7.30, 7.31 y 7.40
- Solution Manager, versión 7.2
- 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 y 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.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 7 notas de seguridad y 6 actualizaciones, siendo 1 de ellas de severidad alta y 13 de criticidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

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

La nota de seguridad calificada como alta se refiere a:

- Los usuarios pueden, en determinadas condiciones, solicitar la modificación de las asignaciones de funciones o privilegios a través de la versión 2 de la interfaz REST de SAP Identity Management, que de otro modo estaría restringida sólo para su visualización. Se ha asignado el identificador CVE-2019-0301 para esta vulnerabilidad.

Los identificadores asignados para el resto de vulnerabilidades son: CVE-2019-0287, CVE-2019-0280, CVE-2019-0298, CVE-2019-0289, CVE-2019-0293, CVE-2019-0291 y CVE-2018-2484.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 16/05/2019

Importancia: Crítica

Recursos afectados:

- Cisco PI Software, versiones anteriores a 3.4.1, 3.5 y 3.6.
- EPN Manager, versiones anteriores a 3.0.1.
- Cisco Aggregation Services Router (ASR) 9000 Series, cuando cumple las siguientes condiciones:
  - El router está ejecutando Cisco IOS XR Software, versión 5.3.3 Service Pack 10.
  - El router tiene la funcionalidad MPLS OAM configurada.
- Cisco Webex Business Suite, todas las versiones anteriores a WBS39.2.205 de Webex Network Recording Player y Webex Player.
- Cisco Webex Meetings Online, todas las versiones anteriores a 1.3.42 de Webex Network Recording Player y Webex Player.
- Cisco Webex Meetings Server, todas las versiones anteriores a 2.8MR3 SecurityPatch2, 3.0MR2 SecurityPatch2, o 4.0 de Webex Network Recording Player.
- Small Business Sx200, Sx300, Sx500, ESW2 Series Managed Switches.
- Small Business Sx250, Sx350, Sx550 Series Switches.
- Firepower:
  - 4100 Series.
  - 9300 Security Appliances.
- MDS 9000 Series Multilayer Switches
- Nexus 1000V:
  - Para Microsoft Hyper-V.
  - Para VMware vSphere.
- Nexus Series Switches:
  - 3000.
  - 6000.
  - 7000.
  - 7700.
  - 9000 en modo *standalone* NX-OS.
- Nexus Platform Switches:
  - 3500.
  - 5500.
  - 5600.
- Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI).
- Nexus 9500 R-Series Switching Platform.
- Cisco IOS XR Software :
  - 32-bit.
  - 64-bit.
- Cisco Video Surveillance Manager, versión 7.12.0, si se está ejecutando en los modos Operations Manager, Media Server, Maps Server, o Federator.

Descripción:

Cisco ha publicado 13 vulnerabilidades, siendo 3 de ellas críticas y el resto de severidad alta.

Solución:

- Cisco ha publicado actualizaciones, en función del producto afectado, que solucionan las vulnerabilidades. Puede acceder a las actualizaciones desde el panel de descargas de software de Cisco.

Detalle:

- Las tres vulnerabilidades de severidad crítica podrían permitir a un atacante remoto obtener la capacidad de ejecutar código arbitrario con privilegios elevados en el sistema operativo subyacente. La primera de ellas, CVE-2019-1821, puede ser explotada por un atacante no autenticado que tenga acceso de red a la interfaz administrativa afectada. En cuanto a la segunda y la tercera, CVE-2019-1822 y CVE-2019-1823, requieren que un atacante tenga credenciales válidas para autenticarse en la interfaz administrativa afectada.
- El resto de vulnerabilidades, de severidad alta, podrían suponer las siguientes acciones en los productos afectados:
  - Denegación de servicio: CVE-2019-1846, CVE-2019-1806, CVE-2019-1858 y CVE-2019-1849.
  - Ejecución arbitraria de código: CVE-2019-1771, CVE-2019-1772 y CVE-2019-1773.
  - Inyección SQL: CVE-2019-1824 y CVE-2019-1825.
  - Divulgación de información: CVE-2019-1717.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Citrix Hypervisor

Fecha de publicación: 16/05/2019

Importancia: Alta

Recursos afectados:

- XenServer 7.6,
- XenServer 7.1 LTSR Cumulative Update 2,
- XenServer 7.0,
- Citrix Hypervisor 8.0.

Descripción:

Citrix ha publicado varias vulnerabilidades que afectan al hardware de algunas CPUs.

Solución:

- Actualizar Citrix Hypervisor.
- Actualización del microcódigo de la CPU mediante el comando: *xl dmesg | grep 'Hardware features:'*
- Desactivar el *hyper-threading* de la CPU (también conocido como *multi-threading* simultáneo). Los pasos para hacerlo se encuentran disponibles en el siguiente documento.

Además, es posible que se necesiten actualizaciones de los sistemas operativos y del *firmware* (BIOS) del sistema *host*, siguiendo las instrucciones de su proveedor.

Detalle:

- Varias vulnerabilidades en el hardware de la CPU podrían permitir que el código sin privilegios que se ejecuta en un núcleo de la CPU, infiera el valor de los datos de memoria pertenecientes a otros procesos, máquinas virtuales o el hipervisor que se está ejecutando, o se ha ejecutado recientemente, en el mismo núcleo de la CPU. Se han reservado los identificadores CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 y CVE-2019-11091 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad DoS en Liferay

Fecha de publicación: 16/05/2019

Importancia: Alta

Recursos afectados:

- Liferay Faces Alloy, entorno Servlet (non-Portlet) 3.0 .

Descripción:

Liferay Faces Alloy permite a los atacantes subir archivos muy grandes que pueden utilizarse en un ataque de denegación de servicio en un entorno Servlet (no Portlet).

Solución:

- Aplicar el parche adecuado en función de la versión afectada, 2.0.2 o 3.0.2.

Detalle:

- Esta vulnerabilidad no afecta a los *portlets* (componentes modulares de las interfaces de usuario gestionadas y visualizadas en un portal web) que utilizan Liferay Faces Alloy. Sin embargo, una vulnerabilidad, recientemente descubierta y corregida (*DoS via large file upload*), hace que la validación *com.liferay.faces.util.uploadedFileMaxSize* también se ignore en un entorno *portlet*.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en WebSphere Application Server de IBM

Fecha de publicación: 16/05/2019

Importancia: Crítica

Recursos afectados:

- WebSphere Application Server ND, versión 9.0
- WebSphere Application Server ND, versión 8.5
- WebSphere Virtual Enterprise, versión 7.0

Descripción:

Ryan Wincey de IBM ha reportado una vulnerabilidad de ejecución remota de código en WebSphere Application Server Network Deployment.

Solución:

La solución recomendada es aplicar el parche provisional, el Fixpack o el PTF que contiene el APAR para cada producto, tan pronto como sea posible.

- Para WebSphere Application Server ND tradicional y WebSphere Application Server ND Hypervisor Edition, versiones desde 9.0.0.0 a 9.0.0.11:
  - actualice a niveles mínimos de fixpack según lo requiera el parche provisional y luego aplique el arreglo provisional PH11655, o
  - aplique el fixpack 9.0.0.12 o posterior (disponibilidad prevista 2Q 2019).
- Para WebSphere Application Server ND tradicional y WebSphere Application Server ND Hypervisor Edition, versiones desde 8.5.0.0 hasta 8.5.5.15:
  - actualice a niveles mínimos de fixpack según lo requiera el parcheo provisional y luego aplique el arreglo provisional PH11655, o
  - aplique el fixpack 8.5.5.16 o posterior (disponibilidad prevista 3Q 2019).
- Para WebSphere Virtual Enterprise Edition v7.0: aplicar el parche provisional PH11655.
  - NOTA: WebSphere Virtual Enterprise V7 está fuera de soporte; IBM recomienda actualizar a una versión, *release* o plataforma soportada del producto.

Detalle:

- IBM WebSphere Application Server ND podría permitir a un atacante remoto ejecutar código arbitrario en el sistema con una secuencia, especialmente diseñada, de objetos serializados de fuentes no confiables. Se ha reservado el indicador CVE-2019-4279

a esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Secuestro de DLL en FortiClient

Fecha de publicación: 17/05/2019

Importancia: Alta

Recursos afectados:

- FortiClient for Windows, versión anterior a la 6.0.6.

Descripción:

Se ha publicado una vulnerabilidad de ruta de búsqueda insegura en el instalador en línea de FortiClient que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema.

Solución:

- Actualizar a FortiClient para Windows versión 6.0.6 o posterior.

Detalle:

- Una vulnerabilidad de ruta de búsqueda insegura en el instalador en línea de FortiClient, podría permitir que un atacante remoto no autenticado, con control sobre el directorio en el que reside FortiClientOnlineInstaller.exe, ejecute código arbitrario en el sistema mediante la carga de archivos.dll maliciosos en ese directorio. Se ha reservado el identificador CVE-2019-5589 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Integrated Lights-Out 4 y 5 de HPE

Fecha de publicación: 20/05/2019

Importancia: Alta

Recursos afectados:

- HPE Integrated Lights-Out 5 (iLO 5) para servidores HPE Gen10, versiones 1.39 y anteriores,
- HPE Integrated Lights-Out 4 (iLO 4), versiones 2.61b y anteriores.

Descripción:

HP ha publicado múltiples vulnerabilidades en sus productos Integrated Lights-Out (iLO) que podrían permitir a un atacante remoto realizar *Cross-Site Scripting* (XSS), inyección de datos no autorizados y desbordamiento del búfer.

Solución:

- Para iLO 4, actualizar a la versión de *firmware* 2.70 o posterior.
- Para iLO 5, actualizar a la versión de *firmware* 1.40a o posterior.

Detalle:

- Las vulnerabilidades en HPE Integrated Lights-Out 4 (iLO 4) para los servidores Gen9 y HPE Integrated Lights-Out 5 (iLO 5) para los servidores Gen10, podrían permitir a un atacante remoto llevar a cabo: ataques *Cross-Site Scripting* (XSS), inyección de datos no autorizados y desbordamiento del búfer. Se han reservado los identificadores CVE-2019-11982, CVE-2019-11983, y se ha asignado CVE-2018-7117 para estas vulnerabilidades.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 20/05/2019

Importancia: Alta

Recursos afectados:

- 3.6 hasta 3.6.3, 3.5 hasta 3.5.5, 3.4 hasta 3.4.8, 3.1 hasta 3.1.17 y versiones anteriores no soportadas.

Descripción:

Se han descubierto 3 vulnerabilidades en la plataforma Moodle, una de criticidad alta y 2 de criticidad baja.

Solución:

- Actualizar a las versiones 3.7, 3.6.4, 3.5.6, 3.4.9 y 3.1.18.

Detalle:

- Un servicio web de mensajería, recupera mensajes que no pertenecen a las conversaciones del usuario y, haciendo uso de la vulnerabilidad de criticidad alta, todas las conversaciones podían ser vistas por el usuario. Se ha reservado el identificador CVE-2019-10132 para esta vulnerabilidad.

Para el resto de vulnerabilidades con criticidad baja, se han reservado los identificadores CVE-2019-10133 y CVE-2019-10134.

Etiquetas: Actualización, CMS, Vulnerabilidad

Escalado de privilegios en IBM MQ

Fecha de publicación: 23/05/2019

Importancia: Alta

Recursos afectados:

- IBM MQ V8
  - versiones 8.0.0.0 - 8.0.0.11
- IBM MQ V9 LTS
  - versiones 9.0.0.0 - 9.0.0.5
- IBM MQ V9.1 LTS
  - versiones 9.1.0.0 - 9.1.0.1
- IBM MQ V9.1 CD
  - versión 9.1.1

Descripción:

Se ha detectado una vulnerabilidad de criticidad alta en IBM MQ, que podría permitir a un atacante ejecutar código con permisos de administrador.

Solución:

Aplicar las siguientes actualizaciones, en función de la versión afectada de IBM MQ:

- IBM MQ V8, 8.0.0.12
- IBM MQ V9 LTS, 9.0.0.6
- IBM MQ V9.1 LTS, 9.1.0.2
- IBM MQ V9.1 CD, 9.1.2

Detalle:

- La vulnerabilidad se debe a una incorrecta configuración de los permisos en los directorios de instalación de IBM MQ, un atacante local sin privilegios podría llegar a ejecutar código con permisos de administrador. Se ha reservado el identificador CVE-2019-4078 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de path transversal en Bitbucket Data Center

Fecha de publicación: 24/05/2019

Importancia: Crítica

Recursos afectados:

Bitbucket Data Center versiones:

- de 6.1.0 hasta 6.1.1
- de 6.0.0 hasta 6.0.2
- de 5.16.0 hasta 5.16.2
- de 5.15.0 hasta 5.15.2
- de 5.14.0 hasta 5.14.3
- de 5.13.0 hasta 5.13.5

Descripción:

Johannes Moritz, de RIPS Technologies, ha descubierto una vulnerabilidad de severidad crítica, del tipo *path transversal* (o incorrecta limitación de rutas de directorios) en la herramienta de migración de Bitbucket Data Center, que puede llevar a la ejecución remota de código en versiones con licencia de Centro de Datos.

Solución:

Atlassian recomienda actualizar a la última versión de Bitbucket Data Center, cuya descripción se puede consultar en las notas de la versión. Puede descargar la última versión de Bitbucket Data Center desde el centro de descargas.

- Actualice Bitbucket Data Center a la versión 6.1.2 o superior.
- Si no puede actualizar a 6.1.2, actualize a las versiones siguientes que contienen parches para solucionar esta vulnerabilidad y están disponibles para su descarga:
  - Si está ejecutando las versiones 6.0.x actualice a la versión 6.0.3
  - Si está ejecutando las versiones 5.16.x actualice a la versión 5.16.3
  - Si está ejecutando las versiones 5.15.x actualice a la versión 5.15.3
  - Si está ejecutando las versiones 5.14.x actualice a la versión 5.14.4
  - Si está ejecutando las versiones 5.13.x actualice a la versión 5.13.6

Detalle:

- Un atacante remoto con usuario autenticado con permisos de administrador puede explotar esta vulnerabilidad de incorrecta limitación de rutas de directorios (*path transversal*) para escribir archivos en ubicaciones arbitrarias, lo que puede llevar a la ejecución remota de código en sistemas que ejecutan una versión vulnerable de Bitbucket Data Center. Las versiones de Bitbucket Server sin licencia del Centro de Datos no son vulnerables. Se ha reservado el CVE-2019-3397 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en FortiOS de FortiGuard

Fecha de publicación: 27/05/2019

Importancia: Alta

Recursos afectados:

FortiOS, versiones:

- Desde 6.0.0 hasta 6.0.4
- Desde 5.6.0 hasta 5.6.8
- Desde 5.4.1 hasta 5.4.10
- Las versiones 5.4.0 e inferiores (incluida la rama 5.2) no se ven afectadas.

Para la vulnerabilidad con identificador CVE-2018-13382, el producto está afectado solo si el portal web SSL VPN está habilitado.

Descripción:

Los investigadores Meh Chang y Orange Tsai, de DEVCORE Security Research Team, han reportado dos vulnerabilidades de salto de directorio y de autorización incorrecta.

Solución:

- Actualizar a versiones de FortiOS 5.4.11, 5.6.9, 6.0.5, 6.2.0 o superiores.

Detalle:

- Una vulnerabilidad de salto de directorio en el portal web FortiOS SSL VPN puede permitir a un atacante no autenticado descargar archivos de sistema FortiOS a través de solicitudes de recursos HTTP, especialmente diseñadas, provocando una divulgación de información. Se ha reservado el identificador CVE-2018-13379 para esta vulnerabilidad.
- Una vulnerabilidad de autorización incorrecta en el portal web SSL VPN puede permitir que un atacante no autenticado cambie la contraseña de un usuario de un portal web SSL VPN a través de solicitudes HTTP, especialmente diseñadas. Se ha reservado el identificador CVE-2018-13382 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 31/05/2019

Importancia: Alta

Recursos afectados:

- La vulnerabilidad de severidad alta afecta a los productos:
  - WAC510, con firmware anterior a 5.0.10.2
- El resto de vulnerabilidades afectan a:
  - D3600 y D6000 con firmware anterior al 1.0.0.75
  - D6100, con firmware anterior al 1.0.0.60
  - D7800, con firmware anterior al 1.0.1.47
  - DM200, con firmware anterior al 1.0.0.61
  - EX2700, con firmware anterior al 1.0.1.48
  - EX6100v2 y EX6150v2 con firmware anterior al 1.0.1.76
  - EX6200v2, con firmware anterior al 1.0.1.72
  - EX8000, con firmware anterior al 1.0.1.180
  - R7500v2, con firmware anterior al 1.0.3.38
  - R7800, con firmware anterior al 1.0.2.58
  - R8900, con firmware anterior al 1.0.4.26
  - R9000, con firmware anterior al 1.0.4.8
  - RAX120, con firmware anterior al 1.0.0.74
  - RBK20 y RBK40, con firmware anterior al 2.3.0.28
  - RBK50, con firmware anterior al 2.3.0.32
  - RBR20, con firmware anterior al 2.3.0.28
  - RBR50, con firmware anterior al 2.3.0.32
  - RBS20 y RBS40 con firmware anterior al 2.3.0.28
  - RBS50, con firmware anterior al 2.3.0.32
  - SRK60, con firmware anterior al 2.2.0.64
  - WAC505, con firmware anterior al 5.0.10.2
  - WAC510, con firmware anterior al 8.0.1.3
  - WN2000RPTv3, con firmware anterior al 1.0.1.32
  - WN3000RPv2, con firmware anterior al 1.0.0.68
  - WN3000RPv3, con firmware anterior al 1.0.2.70
  - WN3100RPv2, con firmware anterior al 1.0.0.66
  - WNDR3700v4, con firmware anterior al 1.0.2.102
  - WNDR4300, con firmware anterior al 1.0.2.104
  - WNDR4300v2 y WNDR4500v3 con firmware anterior al 1.0.0.58

- WNR2000v5, con firmware anterior al 1.0.0.68
- D7800, con firmware anterior al 1.0.1.47
- Insight Cloud, con firmware anterior al Insight 5.6

Descripción:

Netgear ha publicado 13 avisos de seguridad que afectan a sus productos, uno de ellos de severidad alta.

Solución:

- Actualizar a la última versión del firmware.

Detalle:

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

- Divulgación de información sensible (severidad alta).
- Cross-Site Scripting (XSS) almacenado.
- Desbordamiento de pila después de la autenticación.
- Cross-Site Scripting (XSS) reflejado.
- Inyección de comandos tras la autenticación.

Etiquetas: Actualización, Vulnerabilidad