Boletín de octubre de 2018

Avisos Técnicos

Múltiples vulnerabilidades en GSKit usado por el Edge Caching Proxy en WebSphere Application Server de IBM

Fecha de publicación: 03/10/2018

Importancia: Alta

Recursos afectados:

Instalación individual de Edge Caching Proxy de las siguientes versiones de WebSphere Application Server:

- Versión 9.0
- Versión 8.5
- Versión 8.0

Descripción:

IBM ha identificado 7 vulnerabilidades, siendo 1 de severidad alta y 6 de severidad media o baja.

Solución:

IBM ha proporcionado las siguientes soluciones:

- Versiones 9.0.0.0 hasta 9.0.0.8
  - Aplicar el parche temporal 9.0.8 o
  - Aplicar el parche 9 (v.9.0.0.9), o superior
- Versiones 8.5.0.0 hasta 8.5.5.14
  - Aplicar el parche temporal 8.5.5 o
  - Aplicar el parche 15 (v.8.5.5.15), o superior
- Versiones 8.0.0.0 hasta 8.0.0.15
  - Aplicar el parche temporal 8.0.0

Detalle:

La vulnerabilidad de severidad alta es la siguiente:

- IBM GSKit (IBM DB2 para Linux, UNIX y Windows) duplica el estado PRNG a través de las llamadas en el sistema fork() cuando se cargan múltiples instancias ICC. Esto podría derivar en IDs de sesión duplicados o en el riesgo de que se duplique material clave. Se ha asignado el identificador CVE-2018-1426 para esta vulnerabilidad.

Para las demás vulnerabilidades se han asignado los siguientes identificadores: CVE-2018-1447, CVE-2018-1427, CVE-2017-3736, CVE-2017-3732, CVE-2016-0705 y CVE-2016-0702.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 04/10/2018

Importancia: Crítica

Recursos afectados:

- Cisco PI Software, versiones desde la 3.2 hasta la 3.4, anteriores a la primera versión liberada si el servidor TFTP está habilitado

(lo está por defecto).
- Cisco DNA Center, versión 1.1.
- Cisco DNA Center Software, anterior a la versión 1.1.4.
- Cisco Webex Business Suite:
  - WBS31: todas las versiones de Cisco Webex Network Recording Player y versiones anteriores a la WBS31.23 en Cisco Webex Player.
  - WBS32: todas las versiones de Cisco Webex Network Recording Player y versiones anteriores a la WBS32.15.20 en Cisco Webex Player.
  - WBS33: todas las versiones de Cisco Webex Network Recording Player y versiones anteriores a la WBS33.4 en Cisco Webex Player.
- Cisco Webex Meetings:
  - Online: todas las versiones de Cisco Webex Network Recording Player y versiones anteriores a la 1.3.37.
  - Server: todas las versiones de Cisco Webex Network Recording Player anteriores a la 3.0MR2 Patch 1.
- Cisco SD-WAN Solution, versiones anteriores a la 17.2.8 y la 18.3.1 ejecutándose en los siguientes productos:
  - vBond Orchestrator Software.
  - vEdge 100 Series Routers.
  - vEdge 1000 Series Routers.
  - vEdge 2000 Series Routers.
  - vEdge 5000 Series Routers.
  - vEdge Cloud Router Platform.
  - vManage Network Management Software.
  - vSmart Controller Software.
- Cisco HyperFlex Software, versiones anteriores a la 3.5(1a).
- Cisco Firepower Threat Defense (FTD) Software, versiones 6.2.3.x anteriores a la 6.2.3.4, si el registro FTP está habilitado, una regla de control de acceso con una política de archivo FTP asociada también está habilitada y el software se está ejecutando en alguno de los siguientes productos:
  - 3000 Series Industrial Security Appliances (ISAs).
  - ASA 5500-X Series Next-Generation Firewalls.
  - Firepower 2100 Series Security Appliances.
  - Firepower 4100 Series Security Appliances.
  - Firepower 9300 ASA Security Module.
  - Firepower Threat Defense Virtual (FTDv).
- Cisco Firepower System Software ejecutándose en alguno de los siguientes productos:
  - Adaptive Security Appliance (ASA) 5500-X Series con FirePOWER Services.
  - Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls.
  - Advanced Malware Protection (AMP) for Networks, 7000 y 8000 Series Appliances.
  - Firepower 2100 y 4100 Series Security Appliances.
  - FirePOWER 7000 y 8000 Series Appliances.
  - Firepower 9300 Series Security Appliances.
  - FirePOWER Threat Defense for Integrated Services Routers (ISRs).
  - Firepower Threat Defense Virtual.
  - Industrial Ethernet 3000 Series Switches.
  - Next-Generation Intrusion Prevention System (NGIPSv).
  - Virtual Next-Generation Intrusion Prevention System (NGIPSv).
- Cisco Prime Collaboration Provisioning, versiones anteriores a la 12.1.
- Los siguientes productos si están ejecutando una versión vulnerable de Cisco Adaptive Security Appliance (ASA) Software o Cisco Firepower Threat Defense (FTD) Software:
  - ASA 5506-X con FirePOWER Services.
  - ASA 5506H-X con FirePOWER Services.
  - ASA 5506W-X conFirePOWER Services.
  - ASA 5508-X conFirePOWER Services.
  - ASA 5516-X conFirePOWER Services.

Descripción:

Cisco ha publicado 10 vulnerabilidades en varios de sus productos, siendo 3 de severidad crítica y 7 de severidad alta.

Solución:

Cisco ha puesto a disposición de los usuarios diversas actualizaciones en función del producto afectado.

- Panel de descarga de Software Cisco.

Detalle:

Las vulnerabilidades de severidad crítica son las siguientes:

- El servidor web HTTP para Cisco Prime Infrastructure (PI) tiene permisos de directorio sin restricciones que podría permitir que un atacante remoto no autenticado cargue un archivo arbitrario y pueda ejecutar comandos en el nivel de privilegio del usuario *prime*. Se ha reservado el identificador CVE-2018-15379 para esta vulnerabilidad.
- Cisco Digital Network Architecture (DNA) Center podría permitir a un atacante remoto no autenticado eludir la autenticación y tener acceso directo no autorizado a funciones de administración críticas. Se ha reservado el identificador CVE-2018-15386 para esta vulnerabilidad.
- El servicio de administración de identidades del Cisco Digital Network Architecture (DNA) Center podría permitir a un atacante remoto no autenticado eludir la autenticación y tomar el control completo de las funciones de administración de identidades. Se ha reservado el identificador CVE-2018-0448 para esta vulnerabilidad.

Para las vulnerabilidades de criticidad alta se han reservado los siguientes identificadores: CVE-2018-15408, CVE-2018-15409, CVE-2018-15410, CVE-2018-15411, CVE-2018-15412, CVE-2018-15413, CVE-2018-15415, CVE-2018-15416, CVE-2018-15417, CVE-2018-15418, CVE-2018-15419, CVE-2018-15420, CVE-2018-15431, CVE-2018-15387, CVE-2018-15382, CVE-2018-15390, CVE-2018-0455, CVE-2018-15389 y CVE-2018-15383.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad en AirWatch Console de VMware

Fecha de publicación: 08/10/2018

Importancia: Crítica

Recursos afectados:

- AirWatch Console 9.7.x.
- AirWatch Console 9.6.x.
- AirWatch Console 9.5.x.
- AirWatch Console 9.4.x.
- AirWatch Console 9.3.x.
- AirWatch Console 9.2.x.
- AirWatch Console 9.1.x.

Descripción:

Se ha detectado una vulnerabilidad de omisión de autenticación en SAML (Security Assertion Markup Language) que se puede aprovechar durante la inscripción del dispositivo.

Solución:

Desde VMware han publicado una lista de versiones a las que se debe actualizar el producto:

- AirWatch Console 9.7.0.3 o superior.
- AirWatch Console 9.6.0.7 o superior.
- AirWatch Console 9.5.0.16 o superior.
- AirWatch Console 9.4.0.22 o superior.
- AirWatch Console 9.3.0.25 o superior.
- AirWatch Console 9.2.3.27 o superior.
- AirWatch Console 9.1.5.6 o superior.

Detalle:

VMware Workspace ONE Unified Endpoint Management Console (AirWatch Console) contiene una vulnerabilidad de omisión de autenticación en SAML (Security Assertion Markup Language) que podría ser aprovechada durante la inscripción del dispositivo. Esta vulnerabilidad puede permitir que un atacante se haga pasar por una sesión SAML autorizada si la autenticación basada en certificados está habilitada. También es relevante si la autenticación basada en certificados no está habilitada, pero el resultado de la explotación se limita a una divulgación de información en esos casos. Se ha asignado el identificador CVE-2018-6979 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en D-Link para el producto Central WiFi Manager

Fecha de publicación: 08/10/2018

Importancia: Alta

Recursos afectados:

- CWM-100: D-Link Central WiFi Manager versión 1.03 para Windows

Descripción:

D-Link ha publicado 4 vulnerabilidades para el producto Central WifiManager (esta herramienta permite administrar y monitorizar puntos de acceso dentro de una red).

Solución:

D-Link recomienda actualizar a la versión 1.03 R0100 - Beta para corregir estas vulnerabilidades.

Detalle:

Las vulnerabilidades son las siguientes:

- Un atacante, sin necesidad de estar autenticado, podría subir un fichero y ejecutar código arbitrario de forma remota. Para esta vulnerabilidad se ha reservado el identificador CVE-2018-17440.
- Un atacante autenticado podría subir un fichero y ejecutar código arbitrario de forma remota. Para esta vulnerabilidad se ha reservado el identificador CVE-2018-17442.
- Un atacante podría realizar ataques del tipo Cross-Site Scripting a través de los parámetros "sitename" y "addUser". Para estas vulnerabilidades se han reservados los identificadores CVE-2018-17441 y CVE-2018-17443.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en IBM Spectrum LSF

Fecha de publicación: 09/10/2018

Importancia: Alta

Recursos afectados:

- IBM Spectrum LSF versión 10.1
- IBM Spectrum LSF versión 9.1.1
- IBM Spectrum LSF versión 9.1.2
- IBM Spectrum LSF versión 9.1.3

Descripción:

IBM ha encontrado una vulnerabilidad de severidad alta que podría permitir a un atacante la escalada de privilegios en los productos

afectados.

Solución:

IBM recomienda actualizar los productos afectados desde su centro de descargas.

Detalle:

- IBM ha solucionado la vulnerabilidad en Spectrum LSF (Load Sharing Facility) mejorando el archivo ejecutable "eauth" (autenticación externa) que autoriza las credenciales de usuario para evitar ataques mediante la carga previa de la función "getuid". Se ha reservado el identificador CVE-2018-1724 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de octubre de 2018

Fecha de publicación: 10/10/2018

Importancia: Crítica

Recursos afectados:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office y Microsoft Office Services y Web Apps
- ChakraCore
- .NET Core
- PowerShell Core
- SQL Server Management Studio
- Microsoft Exchange Server
- Azure IoT Edge
- Hub Device Client SDK for Azure IoT

Descripción:

La publicación de actualizaciones de seguridad de Microsoft este mes consta de 48 vulnerabilidades, 12 clasificadas como críticas y 36 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:

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

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

---

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 10/10/2018

Importancia: Alta

Recursos afectados:

- Intel® RAID Web Console para Windows, versión 3 y anteriores
- Intel® NUC Firmware Kits, descargado antes del 24 de mayo de 2018
- Intel® Graphics Drivers, versiones anteriores a 10.18.x.5056 (15.33.x.5056), 10.18.x.5057 (15.36.x.5057) y 20.19.x.5058 (15.40.x.5058)
- Intel® Client NVMe, versión 4.0.0.1006 y anteriores.
- Datacenter NVMe, versión 4.0.0.1006 y anteriores.
- Intel® RSTe, versión 4.7.0.2082 y anteriores
- Intel® Server Board S7200AP Family, versiones de firmware anteriores a R01.03.0018
- Intel® Compute Module HNS7200AP Family, versiones de firmware anteriores a R01.03.0018
- Intel® Server Board S7200APR Family, versiones de firmware anteriores a R01.03.0018
- Intel® Compute Module HNS7200APR Family, versiones de firmware anteriores a R01.03.0018

Los siguientes productos con versión de firmware anterior a 00.01.0014 también están afectados:

- Intel® Server Board S2600BP Family
- Intel® Compute Module HNS2600BP Family
- Intel® Server System H2000G Family
- Intel® Server Board S2600WF Family
- Intel® Server System R2000WF Family
- Intel® Server System R1000WF Family
- Intel® Server Board S2600ST Family
- Intel® Server Board S2600BPR Family

- Intel® Compute Module HNS2600BPR Family
- Intel® Server System H2000GR Family
- Intel® Server Board S2600WFR Family
- Intel® Server System R2000WFR Family
- Intel® Server System R1000WFR Family
- Intel® Server Board S2600STR Family

Descripción:

Intel ha publicado varias vulnerabilidades de severidades media y alta, que afectan a varios de sus productos.

Solución:

Actualizar los productos afectados desde: https://downloadcenter.intel.com/es.

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades publicadas podría llegar a realizar alguna de las siguientes acciones:

- Escalada de privilegios
- Denegación de servicio
- Acceso no autorizado a información

Se han reservado los siguientes identificadores para las vulnerabilidades: CVE-2018-12173, CVE-2018-12161, CVE-2018-12158, CVE-2018-12152, CVE-2018-12153, CVE-2018-12154, CVE-2018-12131 y CVE-2018-12172.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de denegación de servicio en VMware

Fecha de publicación: 10/10/2018

Importancia: Alta

Recursos afectados:

- VMware vSphere ESXi (ESXi) cualquier versión y para cualquier plataforma.
- VMware Workstation Pro / Player (Workstation) cualquier versión y para cualquier plataforma.
- VMware Fusion Pro, Fusion (Fusion) cualquier versión de OS X.

Descripción:

VMware ESXi, Workstation y Fusion tienen una vulnerabilidad de denegación de servicio debido a un bucle infinito en un sombreador de renderizado 3D.

Solución:

VMware no ha publicado ningún parche para solucionar el problema, recomienda desactivar la función de aceleración 3D.

- ESXi no lo tiene habilitado de forma predeterminada.
- Workstation y Fusion lo tiene habilitado de forma predeterminada.

Detalle:

- VMware ESXi, Workstation y Fusion tienen una vulnerabilidad de denegación de servicio debido a un bucle infinito en un sombreador de renderizado 3D, por la cual un atacante podría proporcionar un archivo de sombreado especialmente diseñado (ya sea en forma binaria o de texto) para activarla. Esta vulnerabilidad se puede desencadenar desde el invitado de VMware viéndose el host de VMware afectado (lo que hace que el proceso *vmware-vmx.exe* se bloquee en el host). Se ha asignado el identificador CVE-2018-6977 para esta vulnerabilidad.

Etiquetas: VMware, Vulnerabilidad

Actualización de seguridad de SAP de octubre 2018

Fecha de publicación: 10/10/2018

Importancia: Alta

Recursos afectados:

- SAP BusinessObjects Business Intelligence Platform, versiones 4.1 y 4.2.
- SAP Business Client, versión 6.5.
- Proyecto Gardener, versión 0.12.2.
- SAP Plant Connectivity, versiones 15.0, 15.1 y 15.2.
- SAP Records Management, versiones 7.0 a 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50 y 7.51.
- SAP HANA, versiones 1.0 y 2.0.
- SAP Netweaver Application Server para ABAP, versiones desde 7.0 hasta 7.02, 7.30, 7.31, 7.40 y desde 7.50 hasta 7.53.
- SAP BusinessObjects Business Intelligence Platform, versiones 4.10 y 4.20.
- SAP Data Services, versión 4.2.
- SAP Plant Connectivity, versión 15.0.
- SAP BusinessObjects BI Platform Servers (Software Development Kit), versiones 4.1 y 4.2.
- SAP Adaptive Server Enterprise (ASE), versiones 15.7 y 16.0.
- SAP Fiori 1.0 para SAP ERP HCM (Approve Leave Request, versión 2), versión 1.0.
- SAP Fiori 1.0 para SAP ERP HCM (Approve Leave Request, versión 2), versión 1.0.
- SAP Adaptive Server Enterprise (ASE), versiones 15.7 y 16.0.

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 15 notas de seguridad, de las cuales 4 son actualizaciones de notas de seguridad publicadas con anterioridad (repartidas entre una de severidad crítica, 2 de severidad alta y una de severidad media), 1 de severidad crítica, 2 de severidad alta y 8 de severidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de divulgación de información.
- 1 vulnerabilidad de actualizaciones de seguridad para el control del navegador Chromium.
- 1 vulnerabilidad de aislamiento incorrecto de la red.
- 1 vulnerabilidad de denegación de servicio.
- 1 vulnerabilidad de aprovechamiento de privilegios.
- 2 vulnerabilidades de validación incorrecta de XML.
- 3 vulnerabilidades de Cross-Site Scripting.
- 1 vulnerabilidad de divulgación de ruta de archivo.
- 2 vulnerabilidades de Cross-Site Request Forgery.

Las vulnerabilidades más relevantes son las siguientes:

- SAP BusinessObjects BI Suite tiene una vulnerabilidad de divulgación de información. Un atacante puede usarlo para revelar información adicional (datos del sistema, información de depuración, etc.) que le ayudaría a conocer el sistema y planificar otros ataques. Se ha asignado el identificador CVE-2018-2471 para esta vulnerabilidad.
- El proyecto Gardener tiene una vulnerabilidad de aislamiento incorrecto de la red, lo que puede permitir que un atacante actuando como administrador en un *shoot cluster* comprometa el *seed cluster* correspondiente u otros *seed clusters* controlados por este *seed cluster*. Se ha asignado el identificador CVE-2018-2475 para esta vulnerabilidad.
- SAP Plant Connectivity (PCo) tiene una vulnerabilidad de denegación de servicio (DoS) que podría permitir a un atacante finalizar un proceso del componente vulnerable. Se han asignado los identificadores CVE-2018-12585 y CVE-2018-12086 para esta vulnerabilidad.

El resto de identificadores CVE presentes en el informe mensual de octubre de 2018 de SAP son: CVE-2018-2465, CVE-2018-2470, CVE-2018-2472, CVE-2018-2466, CVE-2017-12069, CVE-2018-2467, CVE-2018-2469, CVE-2018-2474, CVE-2018-2474 y CVE-2018-2468.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualización de seguridad 3.8.13 de Joomla!

Fecha de publicación: 10/10/2018

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones desde la 1.5.0 hasta la 3.8.12

Descripción:

Joomla ha publicado una actualización de su CMS, que soluciona varias vulnerabilidades que podrían permitir a un atacante que realizara un CSRF, autorizaciones que requieran privilegios de *admin* u obtener un nivel de acceso no autorizado.

Solución:

Actualizar a la versión 3.8.13 de Joomla!.

Detalle:

Las vulnerabilidades solucionadas son las siguientes, todas en el núcleo de Joomla!:

- Securización contra CSRF en *com_installer*
- Violación de ACL en *com_users* en el proceso de verificación del administrador
- Violación del nivel de acceso en *com_tags*
- Nivel de acceso predeterminado inadecuado para *com_joomlaupdate*
- Securización del formulario de contactos *com_contact*

Se han reservado los siguientes identificadores para las citadas vulnerabilidades: CVE-2018-17858, CVE-2018-17855, CVE-2018-17857, CVE-2018-17856 y CVE-2018-17859.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Juniper

Fecha de publicación: 11/10/2018

Importancia: Alta

Recursos afectados:

- Junos OS múltiples versiones (para ver detalle consulte la sección *Referencias*)
- Junos Space Network Management Platform versiones anteriores a 18.2R1
- Junos Space Security Director versiones anteriores a 17.2R1

Descripción:

Juniper ha publicado 15 vulnerabilidades en varios de sus productos, de las cuales 10 son de severidad alta y 5 de severidad media.

Solución:

Actualizar los productos afectados desde el sitio:

- https://www.juniper.net/support/downloads/

Detalle:

Las vulnerabilidades de severidad alta pueden derivar en:

- **Acceso remoto no autorizado.** Para la vulnerabilidad con el identificador asignado: CVE-2018-0044.
- **Robo de información.** Para la vulnerabilidad con el identificador asignado: CVE-2018-0047.
- **Cross-site Scripting**. Para la vulnerabilidad con el identificador asignado: CVE-2018-0046.
- **Denegación de servicio.** Para las vulnerabilidades con los identificadores asignados: CVE-2018-0043, CVE-2018-0045, CVE-2018-0048, CVE-2018-0049, CVE-2018-0050, CVE-2018-0051 y CVE-2018-0052.

Para las demás vulnerabilidades se han asignado los siguientes identificadores: CVE-2018-0053, CVE-2018-0054, CVE-2018-0055, CVE-2018-0056 y CVE-2018-0057.

Etiquetas: Actualización, Sistema Operativo, Vulnerabilidad

Múltiples vulnerabilidades en IBM WebSphere Application Server de IBM Cloud

Fecha de publicación: 11/10/2018

Importancia: Crítica

Recursos afectados:

Esta vulnerabilidad afecta a las siguientes versiones de IBM WebSphere Application Server:

- Liberty
- Versión 9.0
- Versión 8.5

Descripción:

IBM ha publicado un boletín de seguridad describiendo múltiples vulnerabilidades que afectan a IBM WebSphere Application Server perteneciente a IBM Cloud.

Solución:

Para corregir una instancia de servicio existente, se debe abrir el aviso de la vulnerabilidad específica que aparece listada en la sección *Remediation/Fixes* del boletín de seguridad y, a continuación, aplicar los pasos descritos en dicha sección. Alternativamente, eliminar la instancia de servicio vulnerable y crear una nueva instancia.

Detalle:

Las vulnerabilidades descritas son las siguientes:

- IBM WebSphere Application Server podría permitir a un atacante remoto ejecutar código Java arbitrario a través del conector SOAP (*Simple Object Access Protocol*) con un objeto serializado de fuentes no confiables. Se ha asignado el identificador CVE-2018-1567 para esta vulnerabilidad.
- Apache MyFaces y Oracle Mojarra podrían permitir a un atacante remoto ejecutar código arbitrario en el sistema, causado por una configuración incorrecta de ViewState. Si ViewState está configurado para utilizar información de estado no cifrada, un atacante podría explotar esta vulnerabilidad para ejecutar cualquier código que resida en el *classpath* del servidor.
- Las instalaciones de IBM WebSphere Application Server que utilizan *Form Login* podrían permitir que un atacante remoto realizara ataques de *spoofing*. Se ha asignado el identificador CVE-2018-1695 para esta vulnerabilidad.
- IBM WebSphere Application Server podría proporcionar una seguridad más débil de lo esperado bajo ciertas condiciones. Esto podría resultar en un ataque de downgrade del protocolo TLS. Un atacante remoto podría explotar esta vulnerabilidad para realizar ataques *man-in-the-middle*. Se ha asignado el identificador CVE-2018-1719 para esta vulnerabilidad.
- WebSphere Application Server Liberty podría permitir a un atacante remoto obtener información confidencial, causada por un transporte incorrecto cuando Liberty está configurado para utilizar JASPIC (*Java Authentication SPI for Containers*). Esto puede ocurrir cuando el servidor de aplicaciones está configurado para permitir el acceso en un puerto no seguro (http) y utilizando autenticación JASPIC o JSR375. Se ha asignado el identificador CVE-2018-1755 para esta vulnerabilidad.
- IBM WebSphere Application Server Liberty podría permitir a un atacante remoto obtener información confidencial, causada por el fallo en la encriptación de la comunicación ORB (*Object Request Broker*). Se ha asignado el identificador CVE-2018-1683 para esta vulnerabilidad.
- IBM WebSphere Application Server en IBM Cloud podría permitir a un atacante remoto obtener información confidencial causada por el manejo inadecuado de contraseñas. Se ha asignado el identificador CVE-2018-1838 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en PHP

Fecha de publicación: 15/10/2018

Importancia: Alta

Recursos afectados:

- PHP versiones 7.2.x
- PHP versiones 7.1.x

Descripción:

Se han publicado múltiples vulnerabilidades en PHP para las versiones anteriormente mencionadas.

Solución:

Actualizar PHP según la rama de producto instalada a una de las siguientes versiones:

- PHP versión 7.2.11
- PHP versión 7.1.23

Detalle:

Las actualizaciones solucionan múltiples fallos en las versiones afectadas, incluyendo la corrección de las siguientes vulnerabilidades:

- Excepción incorrecta al usar *ReflectionMethod*.
- *ZendOPcache.MemoryBase* periódicamente borrado por el sistema operativo.
- No se puede construir *xmlrpc* con *expat* (parseador de XML).
- Fallo de segmento en la función de apagado después de un error de límite de memoria.
- *posix_getgrnam* no imprime los detalles del grupo.

Etiquetas: Actualización, PHP, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 15/10/2018

Importancia: Crítica

Recursos afectados:

- IBM Flex System Chassis Management Module (CMM) versión 2PET,
- VRA - Vyatta 5600,
- FileNet Content Manager versiones 5.2.1 y 5.5.0,
- IBM Flex System Chassis Management Module (CMM).

Descripción:

IBM ha publicado varias vulnerabilidades, una crítica, 5 altas y 1 media, que afectan a sus productos y que podrían permitir la obtención de información sensible, la escalada de privilegios, la denegación del servicio o el consumo de memoria.

Solución:

- Para IBM Flex System Chassis Management Module (CMM) versión 2PET e IBM Flex System Chassis Management Module (CMM), descargar la actualización desde http://www.ibm.com/support/fixcentral/
- Para VRA - Vyatta 5600, contactar con IBM Cloud Support para solicitar que la ISO de la release 1801q se envíe a su sistema Vyatta.
- Para FileNet Content Manager versiones 5.2.1 y 5.5.0, instalar la versión 5.2.1.7-P8CPE-IF004 o la versión 5.5.1.0-P8CPE

Detalle:

- La vulnerabilidad de Apache Portable Runtime APR que afecta a IBM Flex System Chassis Management Module, podría permitir a un atacante remoto obtener información sensible mediante el uso de una matriz fuera de límites en las funciones apr_time_exp*(). Al utilizar un valor no válido en el campo mes, un atacante remoto podría explotar esta vulnerabilidad para obtener información confidencial o provocar una denegación de servicio. Se ha asignado el identificador CVE-2017-12613 para esta vulnerabilidad de severidad crítica.

Los identificadores reservados para el resto de vulnerabilidades son: CVE-2018-13405, CVE-2018-5390, CVE-2018-3646, CVE-2018-3620, CVE-2018-1844, CVE-2017-17833.

Etiquetas: Actualización, IBM, Vulnerabilidad

Actualizaciones críticas en Oracle (Octubre 2018)

Fecha de publicación: 17/10/2018

Importancia: Crítica

Recursos afectados:

- Application Management Pack for Oracle E-Business Suite, versiones 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7
- Enterprise Manager Base Platform, versiones 12.1.0.5, 13.2
- Enterprise Manager for MySQL Database, versión 13.2
- Enterprise Manager Ops Center, versiones 12.2.2, 12.3.3
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versiones anteriores a la XCP2352 y anteriores a la XCP3050
- Hyperion BI , versión 11.1.2.4
- Hyperion Common Events, versión 11.1.2.4
- Hyperion Data Relationship Management, versión 11.1.2.4.345
- Hyperion Essbase Administration Services, versión 11.1.2.4
- Instantis EnterpriseTrack, versiones 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Orchestrator, versión 9.2
- JD Edwards EnterpriseOne Tools, versión 9.2
- MICROS Lucas, versión 2.9.5
- MICROS PC Workstation 2015, versiones BIOS anteriores a la 01.3.0.2i
- MICROS Relate CRM Software, versiones 10.8, 11.4

- MICROS Retail-J, versiones 12.1.2, 13.0.0
- MICROS XBRi, versiones 10.5.0, 10.6.0, 10.7.0, 10.8.1, 10.8.2, 10.8.3
- MySQL Connectors, versiones 8.0.12 y anteriores
- MySQL Enterprise Monitor, versiones 3.4.9.4237 y anteriores, 4.0.6.5281 y anteriores, 8.0.2.8191 y anteriores
- MySQL Server, versiones 5.5.61 y anteriores, 5.6.41 y anteriores, 5.7.23 y anteriores, 8.0.12 y anteriores
- Oracle Adaptive Access Manager, versiones 11.1.1.7.0, 11.1.2.3.0
- Oracle Agile Engineering Data Management, versiones 6.1.3, 6.2.0, 6.2.1
- Oracle Agile PLM, versiones 9.3.3, 9.3.4, 9.3.5, 9.3.6
- Oracle Agile Product Lifecycle Management for Process, versión 6.2.0.0
- Oracle API Gateway, versión 11.1.2.4.0
- Oracle Banking Platform, versiones 2.5.0, 2.6.0, 2.6.1, 2.6.2
- Oracle BI Publisher, versiones 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Big Data Discovery, versión 1.6.0
- Oracle Business Intelligence Enterprise Edition, versiones 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Communications Application Session Controller, versiones Prior to 3.7.1M0
- Oracle Communications Instant Messaging Server, versiones prior to 10.0.1
- Oracle Communications Messaging Server, versiones prior to 8.0.2
- Oracle Communications MetaSolv Solution, versión 6.3.0
- Oracle Communications Performance Intelligence Center (PIC) Software, versiones prior to 10.2.1
- Oracle Communications User Data Repository, versiones prior to 12.2.0
- Oracle Configuration Manager, versiones 12.1.2.0.2, 12.1.2.0.5
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c
- Oracle Demantra Demand Management, versiones 7.3.5, 12.2
- Oracle Directory Server Enterprise Edition, versión 11.1.1.7
- Oracle E-Business Suite, versiones 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7
- Oracle Endeca Information Discovery Integrator, versiones 3.1.0, 3.2.0
- Oracle Endeca Information Discovery Studio, versiones 3.1.0, 3.2.0
- Oracle Endeca Server, versiones 7.6.1, 7.7.0
- Oracle Enterprise Repository, versiones 11.1.1.7.0, 12.1.3.0.0
- Oracle Fusion Middleware MapViewer, versiones 12.1.3.0, 12.2.1.3
- Oracle GlassFish Server, versión 3.1.2
- Oracle GoldenGate, versiones 12.1.2.1.0, 12.2.0.2.0, 12.3.0.1.0
- Oracle GoldenGate for Big Data, versiones 12.2.0.1, 12.3.1.1, 12.3.2.1
- Oracle Healthcare Translational Research, versión 3.1.0
- Oracle Hospitality Cruise Fleet Management, versión 9.0
- Oracle Hospitality Cruise Shipboard Property Management System, versión 8.0
- Oracle Hospitality Gift and Loyalty, versión 9.0
- Oracle Hospitality Guest Access, versiones 4.2.0, 4.2.1
- Oracle Hospitality Materials Control, versión 18.1
- Oracle Hospitality Reporting and Analytics, versión 9.0
- Oracle HTTP Server, versión 12.2.1.3
- Oracle Identity Analytics, versión 11.1.1.5.8
- Oracle Identity Management Suite, versiones 11.1.2.3.0, 12.2.1.3.0
- Oracle Identity Manager, versiones 11.1.2.3.0, 12.2.1.3.0
- Oracle iLearning, versiones 6.1, 6.2
- Oracle Insurance Calculation Engine, versiones 10.1.1, 10.2.1
- Oracle Insurance Rules Palette, versiones 10.0, 10.1, 10.2, 11.0, 11.1
- Oracle Java SE, versiones 6u201, 7u191, 8u182, 11
- Oracle Java SE Embedded, versiones 8u18, 8u181
- Oracle JRockit, versión R28.3.19
- Oracle Outside In Technology, versión 8.5.3
- Oracle Real-Time Decision Server, versión 3.2.1
- Oracle Retail Allocation, versiones 15.0, 16.0
- Oracle Retail Assortment Planning, versiones 14.1, 15.0, 16.0
- Oracle Retail Back Office, versiones 13.3, 13.4, 14, 14.1
- Oracle Retail Central Office, versión 14.1
- Oracle Retail Customer Management and Segmentation Foundation, versiones 16.0, 17.0
- Oracle Retail Extract Transform and Load, versiones 13.0, 13.1, 13.2
- Oracle Retail Financial Integration, versiones 13.2, 14.0, 14.1, 15.0, 16.0
- Oracle Retail Integration Bus, versión 14.1.2
- Oracle Retail Invoice Matching, versiones 15.0, 16.0
- Oracle Retail Open Commerce Platform, versiones 5.3, 6.0, 6.0.1
- Oracle Retail Order Broker, versiones 5.0, 5.1, 5.2, 15.0, 16.0
- Oracle Retail Point-of-Service, versiones 13.4, 14.0, 14.1
- Oracle Retail Predictive Application Server, versiones 14.0, 14.1, 15.0, 16.0
- Oracle Retail Returns Management, versión 14.1
- Oracle Retail Sales Audit, versiones 15.0, 16.0
- Oracle Retail Xstore Point of Service, versiones 6.5.12, 7.0.7, 7.1.7, 15.0.2, 16.0.4, 17.0.2
- Oracle Service Bus, versiones 12.1.3.0.0, 12.2.1.3.0
- Oracle Transportation Management, versión 6.3.7
- Oracle Tuxedo, versión 12.1.1.0
- Oracle Virtual Directory, versiones 11.1.1.7.0, 11.1.1.9.0
- Oracle VM VirtualBox, versiones prior to 5.2.20
- Oracle WebCenter Portal, versiones 11.1.1.9.0, 12.2.1.3.0
- Oracle WebCenter Sites, versiones 11.1.1.8.0, 12.2.1.3.0
- Oracle WebLogic Server, versiones 10.3.6.0, 12.1.3.0, 12.2.1.3, anteriores a Docker 12.2.1.3.20180913
- OSS Support Tools, versiones anteriores a la 18.4
- PeopleSoft Enterprise Interaction Hub, versión 9.1.0.0
- PeopleSoft Enterprise PeopleTools, versiones 8.55, 8.56, 8.57
- Primavera Gateway, versiones 15.2, 16.2, 17.12
- Primavera P6 Enterprise Project Portfolio Management, versiones 8.4, 15.1, 15.2, 16.1, 16.2, 18.8, 17.7 - 17.12
- Primavera Unifier, versiones 15.1, 15.2, 16.1, 16.2, 17.1-17.12, 18.1-18.8
- Siebel Applications, versiones 18.7, 18.8, 18.9
- Solaris, versiones 10, 11.3, 11.4
- SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, versiones anteriores a la XCP 1123
- Spatial, versiones 2.0, 2.1, 2.2

Descripción:

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades que afectan a múltiples productos.

Solución:

Esta actualización resuelve un total de 301 vulnerabilidades, algunas de las cuales son críticas. El detalle de las vulnerabilidades resueltas

se puede consultar en el enlace de Oracle de la sección de Referencias.

Detalle:

Aplicar los parches correspondientes según los productos afectados. La información para descargar las actualizaciones puede obtenerse del boletín de seguridad publicado por Oracle.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Vulnerabilidad de lectura fuera de límites en VMware

Fecha de publicación: 17/10/2018

Importancia: Crítica

Recursos afectados:

- VMware vSphere ESXi (ESXi) versiones 6.7, 6.5 y 6.0 en plataforma ESXi.
- VMware Workstation Pro / Player (Workstation) versiones 14.x en cualquier plataforma.
- VMware Fusion Pro, Fusion (Fusion) versiones 10.x en plataforma OS X.

Descripción:

Anonymous y Trend Micro's Zero Day Initiative han informado a VMware de una vulnerabilidad de severidad crítica que podría permitir a un atacante la lectura fuera de límites.

Solución:

VMWare ha publicado los siguientes parches para solucionar esta vulnerabilidad en los productos afectados:

- ESXi 6.7, 6.5 y 6.0.
- Workstation Pro 14.1.3.
- Workstation Player 14.1.3.
- Fusion Pro / Fusion 10.1.3.

Detalle:

VMware ESXi, Workstation y Fusion tienen una vulnerabilidad de lectura fuera de límites en dispositivos SVGA, lo que podría permitir que un usuario invitado ejecutase código en el host. Se ha asignado el identificador CVE-2018-6974 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Evasión de autenticación en librería libssh

Fecha de publicación: 17/10/2018

Importancia: Alta

Recursos afectados:

- Versiones de *libssh* anteriores a 0.8.4 y a 0.7.6

Descripción:

El investigador Peter Winter-Smith de NCC Group ha descubierto una vulnerabilidad en la librería *libssh*, que podría permitir a un atacante que se autenticara sin la introducción de credenciales en sesiones SSH que usen las versiones afectadas de la librería.

Solución:

Actualizar *libssh* a las versiones 0.8.4 o 0.7.6.

Detalle:

El mensaje *SSH2_MSG_USERAUTH_SUCCESS* podría ser presentado al servidor en lugar de *SSH2_MSG_USERAUTH_REQUEST,* pudiendo evadir de esta manera el proceso de autenticación. Se ha reservado el identificador CVE-2018-10933 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en BIG-IP de F5

Fecha de publicación: 18/10/2018

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - Versiones desde 13.0.0 hasta 13.1.1.
  - Versiones desde 12.1.0 hasta 12.1.3.
- BIG-IP APM Clients: versiones desde 7.1.5 hasta 7.1.6.
- BIG-IP Edge Client: versiones desde 7101 hasta 7160.

Descripción:

Se han detectado múltiples vulnerabilidades de criticidad alta y media en varios módulos de productos de la plataforma BIG-IP. Estas vulnerabilidades podrían permitir a un atacante la ejecución de un Cross-Site Scripting (XSS), la inyección de un archivo evitando las comprobaciones de los *endpoints* en el servidor de políticas o la exposición de datos de sesión de otras conexiones de usuarios.

Solución:

F5 ha puesto a disposición de sus usuarios diversas actualizaciones para solucionar las vulnerabilidades según la versión:

- Para versiones pertenecientes a la rama de versiones 14.x, actualizar a la versión 14.0.0.0.
- Para versiones pertenecientes a la rama de versiones 13.x, actualizar a la versión 13.1.1.2.
- Para versiones pertenecientes a la rama de versiones 12.x, actualizar a la versión 12.1.3.7.
- Para versiones pertenecientes a la rama de versiones 7.1.x, actualizar a la versión 7.1.7.
- Para versiones pertenecientes a la rama de versiones 71xx, actualizar a la versión 7170.

Detalle:

Las diferentes vulnerabilidades encontradas son las siguientes:

- Una vulnerabilidad Cross-Site Scripting (XSS) presente en una página no revelada de la utilidad BIG-IP Configuration, podría permitir a un usuario autenticado ejecutar JavaScript para el usuario conectado actualmente. Para aprovechar esta vulnerabilidad, el usuario debe visitar una URL especialmente diseñada que incluya el nombre de host de destino específico. Se ha reservado el identificador CVE-2018-15312 para esta vulnerabilidad.
- Una vulnerabilidad en el APM Edge Client, podría permitir a un atacante inyectar un archivo de biblioteca que será cargado por el servidor de políticas y evitando las comprobaciones de endpoints. El componente de inspección de *endpoints* para plataformas Mac OS X y Linux es vulnerable a este problema. Se ha reservado el identificador CVE-2018-15316 para esta vulnerabilidad.
- Un atacante local podría llevar a cabo un ataque de XSS reflejado en las páginas de la utilidad de configuración BIG-IP a las que acceden otros usuarios. Se ha reservado el identificador CVE-2018-15315 para esta vulnerabilidad.
- Esta vulnerabilidad ocurre cuando se cumplen las siguientes condiciones: el sistema APM BIG-IP está configurado para realizar la autenticación NTLM SSO a servidores backend y, además, un proxy delante del sistema BIG-IP APM multiplexa las conexiones de diferentes usuarios.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en el núcleo de Drupal

Fecha de publicación: 18/10/2018

Importancia: Crítica

Recursos afectados:

- Drupal versiones 7.x y 8.x

Descripción:

Drupal ha publicado un boletín de seguridad que contiene 5 vulnerabilidades que podrían derivar en evasión de autorización para accesos específicos, redirecciones a sitios arbitrarios o ejecución remota de código.

Solución:

Dependiendo de la versión desplegada, se deberá actualizar a una de las siguientes versiones: 7.60, 8.6.2 u 8.5.8.

Detalle:

A continuación se detallan las vulnerabilidades que Drupal ha categorizado como *Critical* según el CMSS de NIST:

- Inyección en *DefaultMailSystem::mail()*. Cuando se envía un correo electrónico, algunas variables no son saneadas correctamente. En concreto, podrían contener argumentos usados en línea de comandos. Esta situación podría derivar en la ejecución remota de código por parte de un atacante.
- Validación de enlaces contextuales. El módulo de estos enlaces no valida suficientemente los solicitados. Esta vulnerabilidad requiere que el atacante tenga un rol con el permiso *access contextual links* y podría derivar en la ejecución remota de código.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

---

Vulnerabilidad en IBM Security Access Manager Appliance

Fecha de publicación: 18/10/2018

Importancia: Alta

Recursos afectados:

- IBM Security Access Manager Appliance versiones 9.0.3.1, 9.0.4.0 y 9.0.5.0

Descripción:

IBM ha publicado una vulnerabilidad que afecta a sus dispositivos IBM Security Access Manager y que podría permitir operaciones no autorizadas

Solución:

- Para las versiones anteriores a la 9.0.5.0, actualizar a la versión 9.0.5-ISS-ISAM-FP0000
- Una vez actualizado, aplicar el 9.0.5.0 Interim Fix 2

Detalle:

- Una vulnerabilidad de seguridad podría permitir operaciones no autorizadas cuando se ejecutan los servicios de Advanced Access Control. Se ha reservado el identificador CVE-2018-1850 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 18/10/2018

Importancia: Alta

Recursos afectados:

- Productos Cisco que ejecutan una versión vulnerable del software Cisco FXOS o NX-OS y tienen habilitado el protocolo LLDP:
  - Firepower 4100 Series Next-Generation Firewall versiones 2.3 y anteriores.
  - Firepower 9300 Security Appliance.
  - MDS 9000 Series Multilayer Switches versiones 6.2 y 5.2
  - Nexus 2000 Series Switches versiones 6.0, 5.1 y 5.0.
  - Nexus 3000 Series Switches versiones 6.0 (2) , 5.0 (3) y 7.0 (3) I7 (3).
  - Nexus 3500 Platform Switches versiones 6.0 (2) y 5.0 (3).
  - Nexus 5500, 5600 y 6000 Platform Switches versiones 6.0, 5.1 y 5.0.
  - Nexus 7000 y 77000 Series Switches versiones 6.1 y 5.2.
  - Nexus 9000 Series Fabric Switches en modo de Infraestructura Centrada en la Aplicación (ACI) versiones 13.2 / 3.2 y anteriores.
  - Unified Computing System (UCS) 6100, 6200 y 6300 Series Fabric Interconnects versiones 4.0, 3.2, 3.1, 2.2 y anteriores.
- Productos Cisco que ejecutan una versión vulnerable del software Cisco NX-OS:
  - Cisco Nexus 5500, 5600, y 6000 Series Switches versiones 7.3 y anteriores.
  - Nexus 3600 Platform Switches versión 7.0 (3) F3 (4).
  - Nexus 9000 Series Switches versión 7.0 (3) I7 (3) en modo independiente.
  - Nexus 9500 R-Series Line Cards and Fabric Modules versión 7.0 (3) F3 (4).
- Cisco WLC versiones 8.7, 8.6, 8.5, 8.4, 8.3, 8.2, 8.1, 8.0 y anteriores.
- Puntos de acceso Cisco con versiones 8.5 y anteriores.

Descripción:

Cisco ha publicado 7 vulnerabilidades en varios de sus productos, siendo todas de severidad alta.

Solución:

Cisco ha puesto a disposición de los usuarios diversas actualizaciones en función del producto afectado.

- Panel de descarga de Software Cisco.

Detalle:

La explotación exitosa de alguna de estas vulnerabilidades podría derivar en:

- Denegación de servicios (DoS).
- Escalada de privilegios.
- Revelación de información.

Se han asignado los siguientes identificadores: CVE-2018-0417, CVE-2018-0441, CVE-2018-0442, CVE-2018-0443, CVE-2018-0456, CVE-2018-0378 y CVE-2018-0395 para estas vulnerabilidades.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

---

Vulnerabilidad en Cisco Webex Meetings Desktop App Update Service

Fecha de publicación: 25/10/2018

Importancia: Alta

Recursos afectados:

- Cisco Webex Meetings Desktop App versiones anteriores a la 33.6.0
- Cisco Webex Productivity Tools versiones 32.6.0 y posteriores, hasta la 33.0.5

Descripción:

Una vulnerabilidad en el servicio de actualización de Cisco Webex Meetings Desktop App para Windows podría permitir a un atacante local autenticado ejecutar comandos arbitrarios como usuario privilegiado.

Solución:

Actualizar Cisco Webex Meetings Desktop App y Cisco Webex Productivity Tools

Detalle:

Una vulnerabilidad de validación insuficiente de los parámetros suministrados por el usuario podría permitir a un atacante invocar el comando *update service* con un argumento especialmente diseñado y conseguir ejecutar comandos arbitrarios con privilegios de usuario de SYSTEM.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Evasión de sandbox en varios plugins de Jenkins

Fecha de publicación: 30/10/2018

Importancia: Alta

Recursos afectados:

- Pipeline: Groovy Plugin
- Script Security Plugin

Descripción:

Se ha publicado un aviso de seguridad que podría permitir a un atacante la evasión de mecanismos de protección proporcionados por la libreria Groovy Sandbox.

Solución:

Actualizar los plugins a las siguientes versiones:

- Pipeline: Groovy Plugin 2.60
- Script Security Plugin 1.48

Detalle:

La biblioteca Groovy Sandbox usada por Script Security Plugin y Pipeline Groovy Plugin no aplica ciertas restricciones del sandbox para finalizar métodos. Esto podría utilizarse para invocar constructores y métodos arbitrarios, evitando así la protección del sandbox.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de F5

Fecha de publicación: 31/10/2018

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, PSM, GTM, Link Controller, PEM, WebAccelerator, Websafe): consultar la sección de *Referencias* para revisar las versiones concretas afectadas.
- Enterprise Manager: versión 3.1.1
- BIG-IQ Centralized Management:
  - Versiones desde 6.0.0 hasta 6.0.1
  - Versiones desde 5.0.0 hasta 5.4.0
  - Versión 4.6.0
- BIG-IQ Cloud y Orchestration: versión 1.0.0
- F5 iWorkflow: versiones desde 2.0.1 hasta 2.3.0

Descripción:

Se han detectado múltiples vulnerabilidades de criticidad alta, media y baja en varios productos como BIG-IP, Enterprise Manager, BIG-IQ Centralized Management, BIG-IQ Cloud y Orchestration y F5 iWorkflow. Estas vulnerabilidades podrían permitir un fallo en la configuración de dispositivos debido a un reinicio de TMM (*Traffic Management Microkernel*), ejecución de ataques de denegación de servicio (DoS), interrupción de tráfico, escalada de privilegios para usuarios administrativos autenticados, eludir restricciones para sobrescribir archivos críticos del sistema, condición de falta de memoria y usuarios con certificados revocados que puedan tener acceso al sistema.

Solución:

F5 ha puesto a disposición de sus usuarios diversas actualizaciones para solucionar estas vulnerabilidades. Los parches pueden encontrarse en su centro de descarga de software.

Detalle:

Las vulnerabilidades de criticidad alta encontradas son las siguientes:

- El sistema BIG-IP falla temporalmente al procesar el tráfico cuando se recupera de un reinicio de *Traffic Management Microkernel* (TMM), y los dispositivos configurados en un grupo pueden fallar. Se ha reservado el identificador CVE-2018-15318 para esta vulnerabilidad.
- La vulnerabilidad permite a los atacantes remotos causar una denegación de servicio (DoS) en el sistema BIG-IP. Se ha reservado el identificador CVE-2018-15317 para esta vulnerabilidad.
- Los patrones de tráfico no revelados pueden llevar a un ataque de denegación de servicio (DoS) para el sistema BIG-IP. La configuración que expone esta vulnerabilidad es la dirección IP propia del sistema BIG-IP, que forma parte de un grupo VLAN y que tiene configurado el bloqueo de puertos con cualquier otra cosa que no sea *allow-all*. Se ha reservado el identificador CVE-2018-15320 para esta vulnerabilidad.
- Un atacante puede ser capaz de interrumpir el tráfico o hacer que el sistema BIG-IP falle afectando a otro dispositivo del grupo. Se ha reservado el identificador CVE-2018-15320 para esta vulnerabilidad.

Para el resto de vulnerabilidades de criticidad media o baja se han reservado los siguientes identificadores: CVE-2018-15327, CVE-2018-15324, CVE-2018-15323, CVE-2018-15322, CVE-2018-15321, CVE-2018-15325 y CVE-2018-15326.

Etiquetas: Actualización, Vulnerabilidad