Boletín de marzo de 2019

Avisos Técnicos

Vulnerabilidad de redirección abierta en varios productos de IBM

Fecha de publicación: 04/03/2019

Importancia: Alta

Recursos afectados:

- IBM InfoSphere Information Governance Catalog, versiones 11.3, 11.5 y 11.7
- IBM InfoSphere Information Server on Cloud, versiones 11.5 y 11.7

Descripción:

IBM InfoSphere Information Server podría permitir a un atacante remoto realizar ataques de *phishing*, utilizando un ataque de redirección abierto.

Solución:

- En ambos productos para la versión 11.7:
  - Actualizar a la versión 11.7.0.2 y después actualizar a la versión 11.7.0.2 Service Pack 1.
- En ambos productos para la versión 11.5:
  - Actualizar a la versión 11.5.0.2 y después actualizar a la versión 11.5 Service Pack 5.
- IBM InfoSphere Information Governance Catalog versión 11.3 actualizar a la versión más reciente.

Detalle:

- IBM InfoSphere Information Server podría permitir a un atacante remoto realizar ataques de *phishing*, utilizando un ataque de redireccionamiento abierto. Al persuadir a una víctima para que visite un sitio web especialmente diseñado, un atacante remoto podría explotar esta vulnerabilidad para falsificar la URL mostrada y redirigir a un usuario a un sitio web malicioso que parecía confiable. Esto podría permitir al atacante obtener información muy delicada o realizar nuevos ataques contra la víctima. Se ha reservado el identificador CVE-2018-1875 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidades en JMeter y Qpid Broker-J de Apache

Fecha de publicación: 04/03/2019

Importancia: Crítica

Recursos afectados:

- JMeter versiones 4.0 y 5.0
- Qpid Broker-J desde la versión 6.0.0 hasta la 7.0.6 y versión 7.1.0

Descripción:

Vulnerabilidades en JMeter y Qpid Broker-J de Apache podrían permitir la ejecución remota de código y el cierre inesperado del servicio.

Solución:

- Para JMeter: actualizar a la última versión (5.1) y usar la la conexión SSL RMI autenticada (habilitada por defecto). Además utilizar la ultima versión de java disponible (desde la 8 hasta la 11).

- Para Apache Qpid Broker-J: actualizar a las versiones 7.0.7 o 7.1.1 o posteriores de Qpid Broker-J.

Detalle:

- Un atacante no autenticado podría establecer una conexión RMI a un servidor de JMeter usando RemoteJMeterEngine y proceder con un ataque usando deserialización de datos no confiables. Esto solo afecta a las pruebas que se ejecutan en modo distribuido. Se ha reservado el identificador CVE-2019-0187 para esta vulnerabilidad.
- Una vulnerabilidad de denegación de servicio en Apache Qpid Broker-J, podría permitir a un atacante no autenticado bloquear la instancia del broker mediante el envío de comandos especialmente diseñados, utilizando versiones del protocolo AMPQ inferiores a 1.0. Se ha reservado el identificador CVE-2019-0200 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 07/03/2019

Importancia: Alta

Recursos afectados:

- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- MDS 9000 Series Multilayer Switches
- Nexus 1000V Switch for Microsoft Hyper-V y Nexus 1000V Switch para VMware vSphere
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches, Nexus 9000 Series ACI Mode Switches que ejecuten versiones anteriores a la 14.0(3d) y Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI)
- Nexus 9500 R-Series Line Cards and Fabric Modules
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Descripción:

Cisco ha publicado 26 vulnerabilidades de criticidad alta que afectan a 47 productos.

Solución:

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

Detalle:

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

- Ejecución de código arbitrario CVE-2019-1613, CVE-2019-1612, CVE-2019-1611, CVE-2019-1610, CVE-2019-1609, CVE-2019-1608, CVE-2019-1607, CVE-2019-1606 y CVE-2019-1618.
- Denegación de servicio (DoS) CVE-2019-1597, CVE-2019-1598,CVE-2019-1617, CVE-2019-1599, CVE-2019-1616 y CVE-2019-1594.
- Ejecución remota de código con privilegios de *root* CVE-2019-1614.
- Verificación incorrecta en la firma de la imagen del SO CVE-2019-1615.
- Escalada de privilegios CVE-2019-1604, CVE-2019-1603,CVE-2019-1596, CVE-2019-1602.
- Acceso no autorizado al sistema de archivos CVE-2019-1601 y CVE-2019-1600.
- Escalada de privilegios mediante la ejecución de código autorizado a otros roles de usuario CVE-2019-1593.
- Ejecución arbitraria de código con privilegios de *root* CVE-2019-1605.
- Escapar del *shell* restringido y ejecución arbitraria de código con privilegios de *root* en el dispositivo afectado CVE-2019-1591.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Divulgación de información de usuario en JasperReports Server de TIBCO

Fecha de publicación: 07/03/2019

Importancia: Crítica

Recursos afectados:

- TIBCO JasperReports Server, versiones 6.4.0, 6.4.1, 6.4.2, y 6.4.3
- TIBCO JasperReports Server, versión 7.1.0
- TIBCO JasperReports Server Community Edition, versiones 7.1.0 y anteriores
- TIBCO JasperReports Server para ActiveMatrix BPM, versiones 6.4.3 y anteriores
- TIBCO Jaspersoft para AWS with Multi-Tenancy, versiones 7.1.0 y anteriores
- TIBCO Jaspersoft Reporting y Analytics para AWS, versiones 7.1.0 y anteriores

Descripción:

TIBCO ha publicado una vulnerabilidad descubierta por Steven Seeley (mr_me), de Source Incite trabajando con Trend Micro Zero Day Initiative, que podría permitir a un atacante no autenticado eludir las verificaciones de autorización de partes de la interfaz HTTP de JasperReports Server.

Solución:

- Para TIBCO JasperReports Server, versiones 6.4.0, 6.4.1, 6.4.2, y 6.4.3: actualizar a la versión 6.4.4 o superior.
- Para TIBCO JasperReports Server, versión 7.1.0: actualizar a la versión 7.1.1 o superior.
- Para TIBCO JasperReports Server Community Edition, versiones 7.1.0 y anteriores: actualizar a la versión 7.1.1 o superior.
- Para TIBCO JasperReports Server para ActiveMatrix BPM, versiones 6.4.3 y anteriores: actualizar a la versión 6.4.4 o superior.
- Para TIBCO Jaspersoft para AWS with Multi-Tenancy, versiones 7.1.0 y anteriores: actualizar a la versión 7.1.1 o superior.
- Para TIBCO Jaspersoft Reporting y Analytics para AWS, versiones 7.1.0 y anteriores: actualizar a la versión 7.1.1 o superior.

Detalle:

- Esta vulnerabilidad, para la que se ha reservado el identificador CVE-2018-18815, podría permitir a un atacante el acceso de lectura no autenticado a los contenidos del sistema host, cuando se combina con la vulnerabilidad identificada por el CVE-2018-18809.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades de desbordamiento de búfer en Db2 de IBM

Fecha de publicación: 08/03/2019

Importancia: Alta

Recursos afectados:

- IBM Db2 V9.7, V10.1, V10.5 y V11.1 en todas las plataformas.

Descripción:

IBM ha publicado múltiples vulnerabilidades de desbordamiento de búfer en sus productos IBM Db2 que podrían permitir a un atacante la escalada de privilegios desde un usuario local autenticado hasta el *root* o el propietario de la instancia.

Solución:

- Aplicar el parche correspondiente en función de la versión y la plataforma. Los enlaces de descarga se encuentran disponibles en la sección de *"Referencias"*.

Detalle:

- IBM DB2 para Linux, UNIX y Windows (incluido DB2 Connect Server) se ve afectado por múltiples vulnerabilidades de desbordamiento de búfer que podrían permitir:
  - Que un atacante ejecute código arbitrario. Se han reservado los identificadores CVE-2018-1922 y CVE-2018-1923 para esta vulnerabilidad.
  - Que un atacante local autenticado ejecute código arbitrario en el sistema como *root*. Se han reservado los identificadores CVE-2018-1978, CVE-2018-1980, CVE-2018-4015 y CVE-2018-4016 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en IBM MQ

Fecha de publicación: 11/03/2019

Importancia: Alta

Recursos afectados:

- IBM MQ V8, versiones 8.0.0.0 - 8.0.0.10
- 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, versiones 9.1.0 - 9.1.1

Descripción:

IBM ha publicado varias vulnerabilidades en IBM MQ que podrían permitir la ejecución de código con privilegios de root y la escalada de privilegios.

Solución:

- IBM MQ V8, aplicar el parche 8.0.0.11
- IBM MQ V9 LTS, aplicar iFix IT27293 para IBM MQ 9.0.0.5
- IBM MQ V9.1 LTS, aplicar iFix IT27293 para IBM MQ 9.1.0.1
- IBM MQ V9.1 CD, aplicar iFix IT24586 para IBM MQ 9.1.1

Detalle:

- IBM WebSphere MQ podría permitir a un atacante local inyectar código con privilegios de root. Se ha reservado el identificador CVE-2018-1998 para esta vulnerabilidad.
- IBM MQ podría permitir a un atacante autenticado la escalada de privilegios al utilizar canales multiplexados. Se ha reservado el identificador CVE-2018-1974 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de divulgación de información en ADM Agent de Citrix

Fecha de publicación: 12/03/2019

Importancia: Crítica

Recursos afectados:

- Citrix Application Delivery Management (ADM) Agent, versión 12.1 anterior al *build* 50.33
- Citrix Application Delivery Management (ADM) Agent Cloud, versión 13.0 anterior al *build* 33.23

Descripción:

Citrix ha detectado una vulnerabilidad de severidad crítica en su producto Application Delivery Management (ADM), que permitiría la obtención de información sensible con la que realizar una escalada de privilegios.

Solución:

Esta vulnerabilidad ha sido solucionada en las siguientes versiones, disponibles en su centro de descargas:

- Citrix Application Delivery Management Agent, versión 12.1 del *build* 50.33 y posteriores.
- Citrix Application Delivery Management Agent Cloud, versión 13.0 del *build* 33.23 y posteriores.

Detalle:

- Se ha identificado una vulnerabilidad en Application Delivery Management Agent (ADM) de Citrix, que podría permitir a un atacante no autenticado con acceso de red a la interfaz del agente de administración, obtener información confidencial. La información divulgada podría ser utilizada para llevar a cabo una escalada de privilegios más allá del agente. Se ha reservado el identificador CVE-2019-9548 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 12/03/2019

Importancia: Alta

Recursos afectados:

- D3600, versiones de *firmware* anteriores a 1.0.0.75
- D6000, versiones de *firmware* anteriores a 1.0.0.75
- D6100, versiones de *firmware* anteriores a 1.0.0.60
- D8500, versiones de *firmware* anteriores a 1.0.3.43
- R6400, versiones de *firmware* anteriores a 1.0.1.44
- R6700, versiones de *firmware* anteriores a 1.0.2.6
- R6900, versiones de *firmware* anteriores a 1.0.2.4
- R6900P, versiones de *firmware* anteriores a 1.3.1.44
- R7000, versiones de *firmware* anteriores a 1.0.9.42
- R7000P, versiones de *firmware* anteriores a 1.3.1.44
- R7100LG, versiones de *firmware* anteriores a 1.0.0.48
- R7300, versiones de *firmware* anteriores a 1.0.0.68
- R7800, versiones de *firmware* anteriores a 1.0.2.62
- R7900P, versiones de *firmware* anteriores a 1.4.1.30
- R8000, versiones de *firmware* anteriores a 1.0.4.28
- R8000P, versiones de *firmware* anteriores a 1.4.1.30
- R8300, versiones de *firmware* anteriores a 1.0.2.128
- R8500, versiones de *firmware* anteriores a 1.0.2.128
- R8900, versiones de *firmware* anteriores a 1.0.4.26
- R9000, versiones de *firmware* anteriores a 1.0.4.26
- WNDR3700v4, versiones de *firmware* anteriores a 1.0.2.102
- WNDR4300, versiones de *firmware* anteriores a 1.0.2.104
- WNDR4300v2, yWNDR4500v3 versiones de *firmware* anteriores a 1.0.0.58
- WNR2000v5, versiones de *firmware* anteriores a 1.0.0.66

Descripción:

Este aviso contiene 11 vulnerabilidades que afectan a productos de Netgear, 4 de las cuales son de severidad alta.

Solución:

- Actualizar a la última versión de firmware disponible en el sitio web.

Detalle:

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

- Inyectar comandos después de la autenticación.
- Desbordar la pila (*stack*) tras la autenticación.
- *Cross-site scripting.*
- Evadir la autenticación.
- Desbordar el búfer tras la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en BIG-IP de F5

Fecha de publicación: 12/03/2019

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) versiones:
  - 14.0.0
  - 13.0.0 hasta 13.1.1
  - 12.1.0 hasta 12.1.4
  - 11.6.1 hasta 11.6.3
  - 11.2.1 hasta 11.5.9
- Entreprise Manager versión 3.1.1

Descripción:

F5 ha publicado varias vulnerabilidades que afectan a sus productos, siendo una de criticidad alta, dos de criticidad media y tres de criticidad baja.

Solución:

- Actualizar BIG-IP (LTM, AAM, AFM, Analytics, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) a las versiones siguientes, según la vulnerabilidad y rama a la que pertenezcan:
  - Rama 14.x actualizar a las versiones 14.0.0, 14.1.0 o 14.0.0.3
  - Rama 13.x actualizar a las versiones 13.0.1, 13.0.0HF, 13.1.0, 13.1.0.8 o 13.1.1.2
  - Rama 12.x actualizar a las versiones 12.0.0, 12.1.3.7, o 12.1.4
  - Rama 11.x actualizar a las versiones 11.6.3.3 o 11.5.9

Detalle:

- La vulnerabilidad de criticidad alta es debida a una corrupción de memoria en TMM (*Traffic Management Microkernel*) cuando procesa mensajes *ClientHello* fragmentados en la sesión DTLS, pudiendo ocasionar un cierre inesperado. Un atacante podría explotar esta vulnerabilidad para generar una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-6596 para esta vulnerabilidad.
- Al resto de vulnerabilidades, de criticidades media y baja, se les han reservado los identificadores: CVE-2019-6599, CVE-2019-6601, CVE-2019-6600, CVE-2019-6598, CVE-2019-6597.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de marzo de 2019

Fecha de publicación: 13/03/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client versión 6.5
- SAP HANA Extended Application Services, versión 1
- SAP NetWeaver Java Application Server (J2EE-APPS), versiones desde 7.10 hasta 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50
- ABAP Server (usado en NetWeaver ySuite/ERP), versión usando Kernel 7.21 o 7.22, ABAP Server 7.00 to 7.31, usando Kernel 7.45, 7.49 or 7.53, ABAP Server 7.40 hasta 7.52 o ABAP Platform
- ABAP Server of SAP NetWeaver y ABAP Platform versiones KRNL32NUC 7.21, KRNL32NUC 7.21EXT, KRNL32NUC 7.22, KRNL32NUC 7.22EXT, KRNL32UC 7.21, KRNL32UC 7.21EXT, KRNL32UC 7.22, KRNL32UC 7.22EXT, KRNL64NUC 7.21, KRNL64NUC 7.21EXT, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64NUC 7.49, KRNL64NUC 7.74, KRNL64UC 7.21, KRNL64UC 7.21EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.49, KRNL64UC 7.73, KRNL64UC 7.74, KRNL64UC 8.04, KERNEL 7.21, KERNEL 7.45, KERNEL 7.49, KERNEL 7.53, KERNEL 7.73, KERNEL 7.74, KERNEL 7.75 y KERNEL 8.04
- ABAP Platform (SLD Registration), versiones - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49; KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73; KERNEL desde 7.21 hasta 7.22, 7.45, 7.49, 7.53, 7.73 y 7.75
- SAP Mobile Platform SDK, versiones anteriores a SDK 3.1 SP03 PL02 y SDK 3.1 SP04
- SAP BusinessObjects Business Intelligence Platform (BI Workspace), versión 4.10 y 4.20
- SAP BusinessObjects Business Intelligence Platform (CMC Module), versión 4.10, 4.20 y 4.30
- SAP Plant Connectivity, versiones - 15.1, 15.2
- SAP Enterprise Financial Services, versiones SAPSCORE 1.13, 1.14 y 1.15 y S4CORE 1.01, 1.02 y 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
- FSAPPL, versión 5
- S4FPSL, versión 1
- Banking services desde SAP, versión 9.0

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 9 notas de seguridad y 3 actualizaciones, siendo 1 de ellas de severidad crítica, 2 altas y 9 de criticidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de falta de comprobación de autorización.
- 2 vulnerabilidades de XSS (*Cross-Site Scripting*).
- 1 vulnerabilidad de denegación de servicio.
- 4 vulenrabilidades *XML External entity*
- 2 vulnerabilidades de otro tipo.

La actualizacion de seguridad calificada como crítica se refiere a:

- Una vulnerabilidad en SAP Business Client podria permitir a un atacante inyectar código en memoria especialmente diseñado, provocando una denegación de servicio o la ejecución remota de código.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.4

Fecha de publicación: 13/03/2019

Importancia: Alta

Recursos afectados:

- Joomla! CMS, versiones desde la 3.0.0 hasta 3.9.3

Descripción:

Joomla! ha publicado una nueva versión que soluciona cuatro vulnerabilidades en su núcleo, 1 de criticidad alta y 3 de criticidad baja. Todas ellas del tipo XSS (*Cross-site scripting*).

Solución:

- Actualizar a la versión 3.9.4

Detalle:

- La vulnerabilidad de criticidad alta, es debida a una falta de comprobación en el ACL (*Access Control List*) en los plugins de muestra, pudiendo permitir a un atacante acceso no autorizado. Se ha asignado el identificador CVE-2019-9713 para esta vulnerabilidad.
- Para el resto de vulnerabilidades se han asignado los identificadores CVE-2019-9714, CVE-2019-9711 y CVE-2019-9714

Etiquetas: Actualización, CMS, Vulnerabilidad

Elevación de privilegios en IBM DB2

Fecha de publicación: 13/03/2019

Importancia: Alta

Recursos afectados:

- IBM DB2 versiones V9.7, V10.1, V10.5, y V11.1 en todas las plataformas.

Descripción:

IBM ha publicado una vulnerabilidad en sus productos IBM DB2 que podrían permitir a un atacante la escalada de privilegios desde un usuario local con bajos privilegios hasta usuario con privilegios *root.*

Solución:

Aplicar el parche correspondiente en función de la versión y la plataforma.

- Para DB2 V11.1 el parche V11.1.4.4 iFix001 está disponible para descarga en IBM Fix Central.
- Para cualquier otra versión vulnerable se puede descargar un parche provisional para cada plataforma en IBM Fix Central según el boletín indicado en el apartado «Referencias».

Detalle:

- IBM DB2 para Linux, UNIX y Windows (incluido DB2 Connect Server) descarga librerías de una ruta no confiable, lo que puede ser aprovechado por un atacante para descargar una librería maliciosa y permitir a un usuario con bajos privilegios escalar privilegios hasta *root*. Se ha reservado el identificador CVE-2019-4094 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 13/03/2019

Importancia: Alta

Recursos afectados:

- D6220, con versiones de firmware anteriores a la 1.0.0.46
- D6400, con versiones de firmware anteriores a la 1.0.0.80

- D7000v2, con versiones de firmware anteriores a la 1.0.0.51
- D8500, con versiones de firmware anteriores a la 1.0.3.42
- DGN2200, con versiones de firmware anteriores a la 1.0.0.58
- DGN2200B, con versiones de firmware anteriores a la 1.0.0.58
- DGN2200v1, con versiones de firmware anteriores a la 1.0.0.58
- EX3700, con versiones de firmware anteriores a la 1.0.0.70
- EX3800, con versiones de firmware anteriores a la 1.0.0.70
- EX6000, con versiones de firmware anteriores a la 1.0.0.30
- EX6100, con versiones de firmware anteriores a la 1.0.2.22
- EX6120, con versiones de firmware anteriores a la 1.0.0.40
- EX6130, con versiones de firmware anteriores a la 1.0.0.22
- EX6150, con versiones de firmware anteriores a la 1.0.0.42
- EX6200, con versiones de firmware anteriores a la 1.0.3.88
- EX7000, con versiones de firmware anteriores a la 1.0.0.66
- EX7500, con versiones de firmware anteriores a la 1.0.0.46
- JNDR3000, con versiones de firmware anteriores a la 1.0.0.24
- R6250, con versiones de firmware anteriores a la 1.0.4.26
- R6300v2, con versiones de firmware anteriores a la 1.0.4.28
- R6400, con versiones de firmware anteriores a la 1.0.1.42
- R6400v2, con versiones de firmware anteriores a la 1.0.2.56
- R6700, con versiones de firmware anteriores a la 1.0.1.46
- R6900, con versiones de firmware anteriores a la 1.0.1.46
- R6900P, con versiones de firmware anteriores a la 1.3.2.34
- R7000, con versiones de firmware anteriores a la 1.0.9.32
- R7000P, con versiones de firmware anteriores a la 1.3.2.34
- R7100LG, con versiones de firmware anteriores a la 1.0.0.46
- R7300DST, con versiones de firmware anteriores a la 1.0.0.68
- R7900, con versiones de firmware anteriores a la 1.0.2.16
- R7900P, con versiones de firmware anteriores a la 1.4.0.10
- R8000, con versiones de firmware anteriores a la 1.0.4.18
- R8000P, con versiones de firmware anteriores a la 1.4.0.10
- R8300, con versiones de firmware anteriores a la 1.0.2.122
- R8500, con versiones de firmware anteriores a la 1.0.2.122
- RBW30, con versiones de firmware anteriores a la 2.1.4.16
- WN2500RPv2, con versiones de firmware anteriores a la 1.0.1.54
- WN3100RP, con versiones de firmware anteriores a la 1.0.0.20
- WNDR3400v3, con versiones de firmware anteriores a la 1.0.1.22
- WNDR4500v2, con versiones de firmware anteriores a la 1.0.0.72
- WNR3500Lv2, con versiones de firmware anteriores a la 1.2.0.54

Descripción:

Netgear ha publicado 4 avisos de seguridad, 2 de severidad alta, 1 media y 1 baja.

Solución:

- Actualizar a la última versión de firmware disponible en el sitio web.

Detalle:

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

- desbordamiento de la pila antes de la autenticación,
- cross-site scripting (XSS) reflejado,
- desbordamiento de búfer tras la autenticación,
- desbordamiento de la pila tras la autenticación.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 13/03/2019

Importancia: Alta

Recursos afectados:

- Intel® CSME, versiones anteriores a 11.8.60, 11.11.60, 11.22.60 o 12.0.20
- Intel® Server Platform Services, versiones anteriores a 4.00.04.383 y 4.01.02.174
- Intel® Trusted Execution Engine, versiones anteriores a 3.1.60 o 4.0.10
- Intel® Graphics Driver para Windows, versiones anteriores a 10.18.x.5059 (también conocida como 15.33.x.5059), 10.18.x.5057 (también conocida como 15.36.x.5057), 20.19.x.5063 (también conocida como 15.40.x.5063) 21.20.x.5064 (también conocida como 15.45.x.5064) y 24.20.100.6373
- *Firmware* incluido en las siguientes generaciones de plataformas:
  - 8th Generation Intel(R) Core™ Processor
  - 7th Generation Intel(R) Core™ Processor
  - Intel(R) Pentium(R) Silver J5005 Processor
  - Intel(R) Pentium(R) Silver N5000 Processor
  - Intel(R) Celeron(R) J4105 Processor
  - Intel(R) Celeron(R) J4005 Processor
  - Intel® Celeron(R) N4100 Processor
  - Intel(R) Celeron® N4000 Processor
  - Intel(R) Server Board
  - Intel(R) Server System
  - Intel(R) Compute Module
- Intel® Matrix Storage Manager, versión 8.9.0.1023 y anteriores.
- Intel® Accelerated Storage Manager en RSTe, versión v5.5 y anteriores.
- Intel® SGX SDK
  - Para Linux, versiones anteriores a 2.2

    - Para Windows, versiones anteriores a 2.1
- Intel® USB 3.0 Creator Utility, todas las versiones.

Descripción:

Intel ha publicado 7 avisos en su centro de seguridad de productos que contienen 40 vulnerabilidades, repartidas en 11 de severidad alta y el resto de severidades media y baja.

Solución:

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

Detalle:

Las vulnerabilidades de severidad alta son:

- Una validación de entrada insuficiente en el subsistema Intel® CSME podría permitir a un usuario privilegiado ejecutar código arbitrario desde el acceso local. Se ha reservado el identificador CVE-2018-12190 para esta vulnerabilidad.
- Un desbordamiento de búfer en el subsistema HECI en Intel(R) CSME podría permitir a un usuario sin autenticación ejecutar código arbitrario desde el acceso físico. Se ha reservado el identificador CVE-2018-12208 para esta vulnerabilidad.
- Un control de acceso insuficiente en Intel(R) Capability Licensing Service podría permitir a un usuario sin privilegios realizar una escalada de privilegios desde el acceso físico. Se ha reservado el identificador CVE-2018-12200 para esta vulnerabilidad.
- Una validación de entrada insuficiente en Intel(R) Active Management Technology (Intel(R) AMT) podría permitir a un usuario no autenticado causar una denegación de servicio a través del acceso de red. Se ha reservado el identificador CVE-2018-12187 para esta vulnerabilidad.
- Una validación de entrada insuficiente en Intel(R) AMT en Intel(R) CSME podría permitir a un usuario no autenticado ejecutar código arbitrario desde el acceso físico. Se ha reservado el identificador CVE-2018-12185 para esta vulnerabilidad.
- Una corrupción de memoria en Kernel Mode Driver en Intel(R) Graphics Driver para Windows podría permitir a un usuario privilegiado ejecutar código arbitrario desde el acceso local. Se ha reservado el identificador CVE-2018-12214 para esta vulnerabilidad.
- Una validación de entrada insuficiente en Kernel Mode Driver en Intel(R) Graphics Driver para Windows podría permitir a un usuario privilegiado ejecutar código arbitrario desde el acceso local. Se ha reservado el identificador CVE-2018-12216 para esta vulnerabilidad.
- Una vulnerabilidad de escalada de privilegios en Platform Sample/Silicon Reference *firmware* Intel(R) Server Board, Intel(R) Server System e Intel(R) Compute Module podría permitir a un usuario privilegiado ejecutar código arbitrario desde el acceso local. Se ha reservado el identificador CVE-2018-12204 para esta vulnerabilidad.
- Una vulnerabilidad de escalada de privilegios en Platform Sample/ Silicon Reference *firmware* para 8th Generation Intel(R) Core™ Processor, 7th Generation Intel(R) Core™ Processor podría permitir a un usuario sin autenticar ejecutar código arbitrario desde el acceso físico. Se ha reservado el identificador CVE-2018-12205 para esta vulnerabilidad.
- Permisos incorrectos en Intel(R) Matrix Storage Manager podría permitir a un usuario autenticado realizar una escalada de privilegios desde el acceso local. Se ha reservado el identificador CVE-2019-0121 para esta vulnerabilidad.
- Permisos incorrectos en el instalador de Intel(R) Accelerated Storage Manager en RSTe podría permitir a un usuario sin autenticar realizar una escalada de privilegios desde el acceso local. Se ha reservado el identificador CVE-2019-0135 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de marzo de 2019

Fecha de publicación: 13/03/2019

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player
- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office y Microsoft Office SharePoint
- ChakraCore
- Team Foundation Server
- Skype for Business
- Visual Studio
- NuGet

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, este mes, consta de 63 vulnerabilidades, 18 clasificadas como críticas y 45 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:

El tipo de vulnerabilidades publicadas se corresponde con las siguientes:

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

Etiquetas: Actualización, Microsoft, Vulnerabilidad

Múltiples vulnerabilidades de productos Cisco

Fecha de publicación: 14/03/2019

Importancia: Crítica

Recursos afectados:

- Cisco Common Services Platform Collector (CSPC), versiones desde 2.7.2 hasta 2.7.4.5, y todas las pertenecientes a 2.8.x que sean anteriores a 2.8.1.2
- Cisco Small Business SPA514G IP Phone que está ejecutando una versión de firmware 7.6.2SR2 o anterior.

Descripción:

Se han detectado 2 vulnerabilidades, de severidad crítica y alta, en los productos Cisco Common Services Platform Collector (CSPC) y Cisco Small Business, respectivamente.

Solución:

- Cisco CSPC, descargar desde el centro de software:
  - Versiones 2.7.x, actualizar a la 2.7.4.6
  - Versiones 2.8.x, actualizar a la 2.8.1.2
- Para Cisco Small Business SPA514G IP Phone, no se ha publicado solución ni se publicará en el futuro, ya que el producto ha entrado en un proceso de *end-of-life* y dejará de tener soporte.

Detalle:

- Una vulnerabilidad en Cisco CSPC podría permitir a un atacante remoto no autenticado acceder a un dispositivo afectado, utilizando una cuenta que tenga una contraseña predeterminada y estática. Esta cuenta no tiene privilegios de administrador. Se ha asignado el identificador CVE-2019-1723 a esta vulnerabilidad.
- Una vulnerabilidad en la implementación del procesamiento del *Session Initiation Protocol* (SIP) en Cisco Small Business SPA514G IP Phone podría permitir que un atacante remoto no autenticado provocase que un dispositivo afectado no respondiese, lo que resultaría en una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0389 a esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en Db2 de IBM

Fecha de publicación: 15/03/2019

Importancia: Alta

Recursos afectados:

- IBM Db2 en todas las plataformas para las versiones:
  - 9.7
  - 10.1
  - 10.5
  - 11.1

Descripción:

Una vulnerabilidad de criticidad alta en Db2 de IBM podría permitir a un atacante la escalada de privilegios con permisos de root.

Solución:

- IBM ha publicado una serie de actualizaciones y parches de seguridad que mitigan la vulnerabilidad en función de la versión y el producto afectado.
  - Versión 9.7 actualizar a la versión 9.7 FP11.
  - Versión 10.1 actualizar a la versión 10.1 FP6.
  - Versión 10.5 actualizar a la versión 10.5 FP10.
  - Versión 11.1 aplicar el parche 11.1.4.4 iFix001.

Detalle:

- La vulnerabilidad se debe a que los binarios cargaban librerías compartidas de una ruta no fiable, pudiendo permitir a un usuario con bajos privilegios, acceso al sistema con privilegios de root. Un atacante podría cargar una biblioteca compartida maliciosa para realizar una escalada de privilegios en el sistema. Se ha reservado el identificador CVE-2019-4094 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Divulgación de información en NonStop SafeGuard de HPE

Fecha de publicación: 15/03/2019

Importancia: Alta

Recursos afectados:

- SAFEGUARD: todas las versiones anteriores a T9750L01^AID o T9750H05^AIH y posteriores cuando el atributo de configuración PASSWORD-PROMPT no está configurado en BLIND.
- STDSEC-STANDARD SECURITY PROD: todas las versiones anteriores a T6533L01^ADU o T6533H05^ADW y posteriores cuando el atributo de configuración PASSWORD-PROMPT no está configurado en BLIND.

Descripción:

HPE ha publicado una vulnerabilidad en su producto NonStop SafeGuard que podría permitir a un atacante la divulgación local de las credenciales.

Solución:

Instalar los SPRs apropiados en función de la versión de lanzamiento:

- L-series:
  - T9750L01^AID (SAFEGUARD), ya disponible
  - T6533L01^ADU (STDSEC-STANDARD SECURITY PROD), ya disponible
- J-series:
  - T9750H05^AIH (SAFEGUARD) - estará disponible en la próxima RVU serie J
  - T6533H05^ADW (STDSEC-STANDARD SECURITY PROD) - estará disponible en la próxima RVU serie J

Detalle:

- Algunos comandos del software NonStop Safeguard y NonStop Standard Security requieren que el nombre de usuario y la contraseña se pasen como parámetros de línea de comandos, lo que puede conducir a una divulgación local de las credenciales. Se ha reservado el identificador CVE-2018-7119 para esta vulnerabilidad.

Etiquetas: HP, Vulnerabilidad

Múltiples vulnerabilidades en VMware

Fecha de publicación: 18/03/2019

Importancia: Alta

Recursos afectados:

- VMware Workstation Pro / Player (Workstation), en las ramas:
  - 15.X en sistemas Windows.
  - 14.X en sistemas Windows.
- VMware Horizon, en las ramas:
  - Horizon 7 (CR) 7.X
  - Horizon 7 (ESB) 7.5.X
  - Horizon 6 6.X

Descripción:

VMware ha detectado tres vulnerabilidades en múltiples productos, siendo dos de las vulnerabilidades de criticidad alta y la restante de criticidad media.

Solución:

VMware ha publicado una serie de actualizaciones que mitigan las vulnerabilidades en función del producto y rama afectada:

- VMware Workstation Pro / Player (Workstation):
  - 15.X en sistemas Windows, aplicar la actualización 15.0.3.
  - 14.X en sistemas Windows, aplicar la actualización 14.1.6.
- VMware Horizon:
  - Horizon 7 (CR) 7.X aplicar el parche 7.8 KB67424.
  - Horizon 7 (ESB) 7.5.X aplicar el parche 7.5.2 KB67401.
  - Horizon 6 6.X aplicar el parche 6.2.8 KB67401.

Detalle:

- Una vulnerabilidad en Workstation, debida a una incorrecta gestión de las rutas, permitiría a un atacante explotar esta vulnerabilidad para acceder al ejecutable VMX, pudiendo permitir el secuestro del sistema y una escalda de privilegios del usuario. Se ha asignado el identificador CVE-2018-5511 para esta vulnerabilidad.
- Una vulnerabilidad en Workstation, debida a una inadecuada gestión de las clases COM, podría permitir a un atacante secuestrar el proceso VMX a través de las clases COM, permitiendo una escalada de privilegios. Se ha reservado el identificador CVE-2019-5512 para esta vulnerabilidad.
- Para la vulnerabilidad de criticidad media, se ha reservado el identificador CVE-2019-5513.

Etiquetas: Actualización, VMware, Vulnerabilidad

Validación insuficiente en backend HTTP remoto de PowerDNS

Fecha de publicación: 19/03/2019

Importancia: Alta

Recursos afectados:

- PowerDNS Authoritative versiones 4.1.6 y anteriores.

Descripción:

Una vulnerabilidad de criticidad alta podría permitir a un atacante remoto generar una condición de denegación de servicio, divulgación de información o falsificación de contenido.

Solución:

- Actualizar a la versión 4.1.7 o 4.0.7

Detalle:

- Un fallo en el backend HTTP remoto de PowerDNS Authoritative Server cuando es empleado el modo *RESTful*, podría permitir a un atacante remoto, a través de la generación de una petición DNS maliciosa, generar una condición de denegación de servicio, falsificación de contenido o divulgación de información. Se ha asignado el identificador CVE-2019-3871 para esta vulnerabilidad

Etiquetas: Actualización, DNS, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 19/03/2019

Importancia: Alta

Recursos afectados:

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

- MSA-19-0004 y MSA-19-0007: 3.6 hasta 3.6.2, 3.5 hasta 3.5.4, 3.4 hasta 3.4.7, 3.1 hasta 3.1.16 y versiones anteriores no soportadas.
- MSA-19-0005: 3.6 hasta 3.6.2, 3.5 hasta 3.5.4 y 3.4 hasta 3.4.7
- MSA-19-0006: 3.6 hasta 3.6.2, 3.5 hasta 3.5.4, 3.4 hasta 3.4.7 y versiones anteriores no soportadas.
- MSA-19-0008: 3.6 hasta 3.6.2 y 3.5 hasta 3.5.4
- MSA-19-0009: 3.6 hasta 3.6.2

Descripción:

Se han descubierto 6 vulnerabilidades en la plataforma Moodle, 3 de criticidad alta y 3 de criticidad baja.

Solución:

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

- MSA-19-0004 y MSA-19-0007: 3.6.3, 3.5.5, 3.4.8 y 3.1.17
- MSA-19-0005 y MSA-19-0006: 3.6.3, 3.5.5 y 3.4.8
- MSA-19-0008: 3.6.3 y 3.5.5
- MSA-19-0009: 3.6.3

Detalle:

Las vulnerabilidades de criticidad alta son las siguientes:

- Los usuarios con la capacidad de *login as other users* (como administradores) pueden acceder a los *dashboards* de otros usuarios, pero el JavaScript que esos otros usuarios pueden haber añadido a su *dashboard* no se escapaba cuando era visto por el usuario que iniciaba sesión en su nombre. Se ha reservado el identificador CVE-2019-3847 para esta vulnerabilidad.
- Los permisos no se comprobaron correctamente antes de cargar la información de eventos en la ventana emergente modal de edición de eventos del calendario, de modo que los usuarios no invitados que hayan iniciado sesión pueden ver eventos de calendario no autorizados. (Nota: Era un acceso de sólo lectura, los usuarios no podían editar los eventos). Se ha reservado el identificador CVE-2019-3848 para esta vulnerabilidad.
- Los usuarios pueden asignarse un rol superior al que les corresponde dentro de los cursos o contenidos a los que se accede a través de LTI (*Learning Tools Interoperability*), modificando la solicitud al sitio web del editor de LTI. Se ha reservado el identificador CVE-2019-3849 para esta vulnerabilidad.

Para el resto de vulnerabilidades con criticidad baja, se han asignado los identificadores CVE-2019-3850, CVE-2019-3851 y CVE-2019-3852.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de Cross-Site Scripting en el core de Drupal

Fecha de publicación: 21/03/2019

Importancia: Media

Recursos afectados:

- Versiones 8.6.x anteriores a 8.6.13
- Versiones 8.5.x anteriores a 8.5.14
- Versiones 7.x anteriores a 7.65

Descripción:

Se ha descubierto una vulnerabilidad de *Cross-Site Scripting* (XSS) en el *core* de Drupal.

Solución:

- Para Drupal 8.6, actualizar a la versión 8.6.13

- Para Drupal 8.5 y anteriores, actualizar a la versión 8.5.14
- Para Drupal 7, actualizar a la versión 7.65

Las versiones de Drupal 8 anteriores a 8.5.x están en fase *end-of-life* y, por lo tanto, no reciben actualizaciones de seguridad.

Detalle:

- Bajo ciertas circunstancias, el módulo/subsistema de archivos permite que un usuario malicioso cargue un archivo que puede desencadenar una vulnerabilidad de *Cross-Site Scripting* (XSS).

Etiquetas: CMS, Vulnerabilidad

Múltiples vulnerabilidades en teléfonos IP de Cisco

Fecha de publicación: 21/03/2019

Importancia: Alta

Recursos afectados:

Teléfonos IP de Cisco que ejecuten el software SIP en las versiones anteriores a las siguientes:

- 10.3(1)SR5 para Unified IP Conference Phone 8831
- 11.0(4)SR3 y 11.0(5) para Wireless IP Phone 8821 y 8821-EX
- 12.5(1)SR1 para IP Conference Phone 8832, las series IP Phone 8800 e IP Phone 7800

Descripción:

Cisco ha detectado 5 vulnerabilidades de criticidad alta que afectan a varios de sus teléfonos IP.

Solución:

- Cisco ha puesto a disposición de sus usuarios una serie de actualizaciones que mitigan las vulnerabilidades en función de la versión y producto afectado. Puede descargarse la actualización desde el centro de software de Cisco.

Detalle:

Las vulnerabilidades encontradas podrían permitir a un atacante remoto sin autenticación realizar:

- Modificación no autorizada de archivos.
- Generar una condición de denegación de servicio (*DoS).*
- Eludir comprobaciones de autenticación.
- Acceder a servicios críticos.
- Ejecución arbitraria de código.
- Obtención de privilegios.

Se han reservado los identificadores CVE-2019-1764, CVE-2019-1716, CVE-2019-1763, CVE-2019-1766, CVE-2019-1765 para estas vulnerabilidades.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad en API Connect de IBM

Fecha de publicación: 22/03/2019

Importancia: Alta

Recursos afectados:

- IBM API Connect desde la versión 2018.1 hasta 2018.4.1.2.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta en IBM API Connect 2018.

Solución:

- Actualizar IBM Connect a la versión 2018.4.1.3

Detalle:

- Un atacante sin autenticación, aprovechando la API de IBM Connect, podría obtener *IDs* de acceso de los usuarios registrados. Se ha reservado el identificador CVE-2019-4052 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de F5

Fecha de publicación: 22/03/2019

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), las siguientes versiones:
  - 14.0.0
  - Desde 13.0.0 hasta 13.1.1
  - 12.0.x
  - Desde 12.1.0 hasta 12.1.3
  - Desde 11.2.1 hasta 11.6.3
- BIG-IP (ASM), las siguientes versiones:
  - Desde 14.0.0 hasta 14.0.0.2
  - Desde 13.0.0 hasta 13.1.1.3
  - Desde 12.1.0 hasta 12.1.3
  - Desde 11.6.1 hasta 11.6.3 y desde 11.5.1 hasta 11.5.8

Descripción:

Se han detectado múltiples vulnerabilidades, concretamente 3 con criticidad alta, 3 con media y 1 con baja, en varios productos de F5. Estas vulnerabilidades podrían provocar interrupción remota del servicio, respuesta HTTP inconsistente, parada en el procesamiento del tráfico, *cross-site scripting* (XSS) o consumo excesivo de memoria.

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:

- Los paquetes TCP mal formados enviados a una dirección IP propia o a un servidor virtual FastL4 pueden causar una interrupción del servicio. Este problema afecta a los servidores virtuales del plano de datos y a las propias IP. Se ha reservado el identificador CVE-2019-6603 para esta vulnerabilidad.
- La utilidad de configuración de la página de *login* devuelve una respuesta HTTP inconsistente cuando se procesan solicitudes modificadas, lo que puede proporcionar pistas a un atacante que busca explotar vulnerabilidades en el sistema. Se ha reservado el identificador CVE-2019-6602 para esta vulnerabilidad.
- Bajo ciertas condiciones, los sistemas de hardware con un HSB (*High-Speed Bridge*) que utilizan configuraciones de reenvío de Capa 2 no predeterminadas, pueden experimentar un bloqueo del HSB. El sistema BIG-IP detiene el tráfico de procesamiento, lo que finalmente conduce a una conmutación por error a otro *host* del grupo de alta disponibilidad. Se ha reservado el identificador CVE-2019-6604 para esta vulnerabilidad.

Para el resto de vulnerabilidades de criticidad media o baja, se han reservado los siguientes identificadores: CVE-2019-6607, CVE-2019-6605, CVE-2019-6606 y CVE-2019-6608.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en PuTTY

Fecha de publicación: 25/03/2019

Importancia: Crítica

Recursos afectados:

- Versión 0.70 y anteriores.

Descripción:

PuTTY ha publicado múltiples vulnerabilidades de las cuales 3 son de severidad crítica.

Solución:

- Actualizar a la versión 0.71.

Detalle:

Las vulnerabilidades de severidad crítica son:

- Unix PuTTY utiliza *select(2)* para ver los descriptores de los archivos Unix, ya que contienen una variable del tipo *fd_set* sin límites. Si se encontrase con un archivo con una longitud igual o mayor a 1024 en *fd_set*, el monitor sería incapaz de monitorizar este archivo, produciéndose un desbordamiento de búfer. Se ha asignado el identificador CVE-2019-9895 para esta vulnerabilidad.
- Cuando un usuario ejecuta la ayuda online en el marco de las herramientas de interfaz gráfica de PuTTY, el software intenta encontrar su propio archivo de ayuda al mismo tiempo que su propio ejecutable. Este comportamiento es, precisamente, el que permitiría a un hipotético atacante engañar a la víctima para ejecutar código malicioso en el cliente mediante el secuestro del archivo CHM. Se ha asignado el identificador CVE-2019-9896 para esta vulnerabilidad.
- Un error reside en el modo en que los números criptográficos pseudoaleatorios son generados en PuTTY, que ocasionalmente parece utilizar dos veces el mismo lote de números pseudoaleatorios. Se ha asignado el identificador CVE-2019-9898 para esta vulnerabilidad.

El resto de vulnerabilidades son:

- Ejecución de código vía CHM hijacking.
- Vulnerabilidad de tipo Integer Overflow. Se ha asignado el identificador CVE-2019-9894 para esta vulnerabilidad.
- Denegación de servicio. Se ha asignado el identificador CVE-2019-9897 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de denegación de servicio en

Apache Tomcat

Fecha de publicación: 26/03/2019

Importancia: Alta

Recursos afectados:

- Apache Tomcat®, versiones:
  - Desde la 8.5.0 hasta la 8.5.37
  - Desde la 9.0.0.M1 hasta la 9.0.14

Descripción:

Michal Karm Babacek, de Red Hat, ha descubierto una vulnerabilidad que provoca una condición de denegación de servicio.

Solución:

- Actualizar a la versión 8.5.38 o superior.
- Actualizar a la versión 9.0.16 o superior.

Detalle:

- La implementación de HTTP/2 acepta la apertura consecutiva de un número excesivo de paneles de configuración (SETTINGS) y permite a los clientes mantenerlos abiertos sin leer/escribir datos de solicitud/respuesta. Al mantenerlos abiertos para peticiones que utilizan la API de bloqueo de E/S del *Servlet*, los clientes pueden provocar que los subprocesos en ejecución del lado del servidor se bloqueen, originando un agotamiento de subprocesos y una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-0199 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Vulnerabilidad XXE en Sterling B2B Integrator de IBM

Fecha de publicación: 27/03/2019

Importancia: Alta

Recursos afectados:

- IBM Sterling B2B Integrator, versión 6.0.0.0

Descripción:

Se ha detectado una vulnerabilidad de criticidad alta de tipo *XML External Entity Injection* (XXE) en el producto Sterling B2B Integrator Standard Edition.

Solución:

- Descargar la versión 6.0.0.1 de IBM Sterling B2B Integrator.

Detalle:

- IBM Sterling B2B Integrator Standard Edition es vulnerable a un ataque de tipo *XML External Entity Injection* (XXE) al procesar datos XML. Un atacante remoto podría explotar esta vulnerabilidad para revelar información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2019-4043 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de TIBCO

Fecha de publicación: 27/03/2019

Importancia: Alta

Recursos afectados:

- TIBCO Data Science para AWS, versiones 6.4.0 y anteriores.
- TIBCO Spotfire Data Science, versiones 6.4.0 y anteriores.

Descripción:

TIBCO ha publicado 3 vulnerabilidades que afectan a varios de sus productos, en las que un atacante podría obtener acceso con privilegios al componente del servidor web, modificar o eliminar datos y realizar una suplantación de identidad.

Solución:

- TIBCO Data Science para AWS, actualizar a la versión 6.4.1 o superior.
- TIBCO Spotfire Data Science, actualizar a la versión 6.4.1 o superior.

Detalle:

La explotación exitosa de alguna de estas vulnerabilidades podría permitir a un usuario:

- Mediante *cross-site scripting* (XSS) obtener acceso a todas las capacidades de la interfaz web disponibles para los usuarios con

privilegios. Se ha asignado el identificador CVE-2019-8987 para esta vulnerabilidad.
- Escalar sus privilegios en el sistema afectado, de manera que podría modificar y eliminar datos protegidos. Se ha asignado el identificador CVE-2019-8988 para esta vulnerabilidad.
- Falsificar su cuenta y realizar una suplantación de identidad. Se ha asignado el identificador CVE-2019-8989 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Tableau Desktop

Fecha de publicación: 27/03/2019

Importancia: Alta

Recursos afectados:

- Tableau Desktop para sistemas operativos Mac y Windows:
  - desde la versión 10.1 hasta 10.1.22
  - desde la versión 10.2 hasta 10.2.18
  - desde la versión 10.3 hasta 10.3.18
  - desde la versión 10.4 hasta 10.4.14
  - desde la versión 10.5 hasta 10.5.13
  - desde la versión 2018.1 hasta 2018.1.10
  - desde la versión 2018.2 hasta 2018.2.7
  - desde la versión 2018.3 hasta 2018.3.4
  - desde la versión 2019.1 hasta 2019.1.0 (2019.1.1 fue un lanzamiento de Tableau Server paralizado)
  - desde la versión 2019.1 hasta 2019.1.1

Descripción:

Tableau ha publicado tres vulnerabilidades que afectan a Tableau Desktop que podrían permitir ejecución remota de código y mostrar datos a usuarios no autorizados.

Solución:

- Tableau Desktop ha publicado una serie de actualizaciones que mitigan las vulnerabilidades en función de la versión y sistemas operativos. Puede comprobar la versión en el siguiente listado:
  - version 10.1.23
  - versión 10.2.19
  - versión 10.3.19
  - versión 10.4.15
  - versión 10.5.14
  - versión 2018.1.11
  - versión 2018.2.8
  - versión 2018.3.5
  - versión 2019.1.2

Detalle:

- Una vulnerabilidad permite la revelación de información en *thumbnails* (imágenes en miniatura). Un usuario que pueda verlas en un libro de trabajo, podrá ver una imagen estática del mismo, tal y como existía en el momento en el que se publicó. Estas imagen podría contener datos que el usuario «espectador» no tiene permiso para ver.
- Un usuario que se conecta a un Conector de Datos Web malicioso con Tableau Desktop en Mac puede provocar una vulnerabilidad de corrupción de memoria. Un atacante que explote esta vulnerabilidad podría ejecutar código arbitrario o provocar un bloqueo.
- Cuando se utiliza el protocolo NTLM para autenticarse en un sitio web, existe la posibilidad de una lectura y escritura fuera de los límites. Esto podría provocar la ejecución remota de código o un bloqueo. Abrir un libro malicioso o conectarse a una instancia maliciosa de Tableau Server puede provocar esta vulnerabilidad. Esta vulnerabilidad relacionada con la librería «libcurl» tiene asignados los CVE-2018-16890 y CVE-2019-3822 .

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en BIG-IQ Centralized Management de F5

Fecha de publicación: 28/03/2019

Importancia: Alta

Recursos afectados:

- BIG-IQ Centralized Management, versiones desde 5.0.0 hasta 5.1.0.

Descripción:

F5 ha descubierto una vulnerabilidad con severidad alta que afecta a su producto BIG-IQ Centralized Management.

Solución:

- Actualizar BIG-IQ Centralized Management a la versión 5.2.0 desde el centro de descargas de software.

Detalle:

- Se ha detectado una vulnerabilidad de tipo *XML External Entity* (XXE) en la librería *libexpat* 2.2.0 y anteriores, que permitiría a los atacantes provocar un bucle infinito en el analizador XML, utilizando una declaración de entidad externa malformada desde un DTD (Definición de Tipo de Documento) externo. Se ha asignado el identificador CVE-2017-9233 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 28/03/2019

Importancia: Alta

Recursos afectados:

- Cisco IOS o IOS XE Software:
  - con la función web server habilitada.
  - con Cisco Plug-and-Play (PnP) habilitado e inicializado.
  - configurado para operaciones NBAR.
  - configurado con NAT64 (*Stateless* o *Stateful*), Mapping de Address y Port Using Translation (MAP-T), o Mapping de Address y Port Using Encapsulation (MAP-E).
  - configurado con una interfaz ISDN (RDSI).
  - configurado para operaciones IP SLA.
  - configurado para usar la función Cisco ETA.
- Switches Cisco Catalyst 4500/4500X Series.
- Sierra Wireless WWAN cellular interface con:
  - Cisco IOS Software Release 15.8(3)M.
  - Cisco IOS XE Software Release 16.10.1.
- Cisco ASR 900 RSP3 que ejecutan el software Cisco IOS XE y están configurados para OSPFv2 routing y OSPF Message Digest 5 (MD5) cryptographic authentication.

Descripción:

Cisco ha publicado 23 vulnerabilidades, siendo 17 de ellas de severidad alta y 6 de criticidad media.

Solución:

- Cisco ha publicado diversas 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 vulnerabilidades de severidad alta son las siguientes, con sus correspondientes identificadores asignados:

- Divulgación de información: CVE-2019-1742.
- Inyección de comandos: CVE-2019-1745, CVE-2019-1756 y CVE-2019-1755.
- Denegación de servicio: CVE-2019-1747, CVE-2019-1749, CVE-2019-1738, CVE-2019-1739, CVE-2019-1740, CVE-2019-1751, CVE-2019-1752, CVE-2019-1737, CVE-2019-1750, CVE-2019-1741 y CVE-2019-1746.
- Validación de certificado insuficiente: CVE-2019-1748.
- Escalada de privilegios: CVE-2019-1754 y CVE-2019-1753.
- Subida de ficheros arbitrarios: CVE-2019-1743.

Para las vulnerabilidades de severidad media, se han asignado los siguientes identificadores: CVE-2019-1760, CVE-2019-1758, CVE-2019-1757, CVE-2019-1762, CVE-2019-1761 y CVE-2019-1759

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en la librería GnuTLS

Fecha de publicación: 28/03/2019

Importancia: Alta

Recursos afectados:

- Librería GnuTLS versiones desde la 3.5.8 y anteriores a la 3.6.7.

Descripción:

Se han detectado dos vulnerabilidades de criticidad alta, una de ellas encontrada por el investigador Travis Ormandy de Google Project Zero. Un atacante podría generar un cierre inesperado del servidor o comprometer los certificados.

Solución:

- Actualizar GnuTLS a la versión 3.6.7 o posteriores.

Detalle:

- Un atacante que envíe un mensaje TLS1.3 asíncrono, mal formado, podría generar un cierre inesperado del servidor a través de un acceso no válido al puntero. Se ha reservado el identificador CVE-2019-3836 para esta vulnerabilidad.
- Una corrupción de memoria debida a una doble liberación (*double free*) en la API de verificación de certificados podría comprometer los mismos. Cualquier aplicación, cliente o servidor, que verifique certificados X.509, está afectada. Se ha asignado el identificador CVE-2019-3829 para esta vulnerabilidad.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad

Múltiples vulnerabilidades en productos de

VMware

Fecha de publicación: 29/03/2019

Importancia: Crítica

Recursos afectados:

- VMware vCloud Director for Service Providers (vCD), versión 9.5.x;
- VMware vSphere ESXi (ESXi), versiones 6.0, 6.5 y 6.7 en cualquier plataforma;
- VMware Workstation Pro / Player (Workstation), versiones 14.x y 15.x en cualquier plataforma;
- VMware Fusion Pro / Fusion (Fusion), versiones 10.x y 11.x en OSX.

Descripción:

VMware ha publicado 5 vulnerabilidades que afectan a varios de sus productos.

Solución:

- VMware vCloud Director para proveedores de servicios (vCD), actualizar a la versión 9.5.0.3;
- VMware vSphere ESXi (ESXi):
  - para la versión 6.0, aplicar el parche ESXi600-201903001
  - para la versión 6.5, aplicar el parche ESXi650-201903001
  - para la versión 6.7, aplicar el parche ESXi670-201903001
- VMware Workstation Pro (Workstation):
  - para las versiones 14.x, actualizar a 14.1.7
  - para las versiones 15.x, actualizar a 15.0.4
- VMware Workstation Player (Workstation):
  - para las versiones 14.x, actualizar a 14.1.7
  - para las versiones 15.x, actualizar a 15.0.4
- VMware Fusion Pro / Fusion (Fusion):
  - para las versiones 10.x, actualizar a la versión 10.1.6
  - para las versiones 11.x, actualizar a la versión 11.0.3

Detalle:

- VMware vCloud Director para proveedores de servicio contiene una vulnerabilidad de secuestro de sesión remota en los portales *Tenant* y *Provider*. La explotación de esta vulnerabilidad podría permitir a un atacante malicioso acceder a dichos portales, haciéndose pasar por un usuario con la sesión iniciada en ese momento. Se ha reservado el identificador CVE-2019-5523 para esta vulnerabilidad.
- Un atacante con acceso a una máquina virtual en VMware ESXi, Workstation o Fusion que disponga de un controlador USB 1.1 virtual, podría explotar una vulnerabilidad de lectura/escritura fuera de límites o una de *Time-of-check Time-of-use* (TOCTOU), que le permitiría ejecutar código en el *host*. Se han reservado los identificadores CVE-2019-5518 y CVE-2019-5519 para estas vulnerabilidades.
- VMware Workstation y Fusion tienen una vulnerabilidad de escritura fuera de límites en el adaptador de red virtual e1000, que podría permitir a un atacante ejecutar código en el *host*. Se ha reservado el identificador CVE-2019-5524 para esta vulnerabilidad.
- VMware Workstation y Fusion tienen una vulnerabilidad de escritura fuera de límites en los adaptadores de red virtuales e1000 y e1000e, que podría permitir a un atacante ejecutar código en el *host,* aunque es más probable que resulte en una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-5515 para esta vulnerabilidad.
- VMware Fusion tiene una vulnerabilidad de falta de autenticación en las API a las que se puede acceder a través de un *web socket.* Un atacante podría explotar esta vulnerabilidad engañando al usuario del *host* para que ejecute un JavaScript con el fin de realizar funciones no autorizadas en el equipo invitado en el que está instalado VMware Tools. Se ha reservado el identificador CVE-2019-5514 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Control de acceso inadecuado en WebAccess de Advantech

Fecha de publicación: 29/03/2019

Importancia: Crítica

Recursos afectados:

- WebAccess

Descripción:

El investigador Mat Powell, de Trend Micro Zero Day Initiative, ha reportado dos vulnerabilidades de control de acceso inadecuado, que afectan al software WebAccess de Advantech. Un atacante remoto podría ejecutar código arbitrario en el dispositivo sin estar autenticado.

Solución:

- No se ha publicado ninguna solución para estas vulnerabilidades. Se aconseja restringir la interacción únicamente a máquinas de confianza. Solo se debe permitir la comunicación con WebAccess a clientes y servidores relacionados de forma legítima en el proceso.

Detalle:

- Se ha detectado una falta de validación de la cadena de texto proporcionada por el usuario, en los servicios *spchapi.exe* y *tv_enua.exe*, antes de utilizarse para ejecutar una llamada al sistema. Un atacante remoto no autenticado podría ejecutar código arbitrario en el contexto de Administrador.

Etiquetas: 0day, Vulnerabilidad