Boletín de enero de 2019

Avisos Técnicos

Boletín de seguridad de Microsoft de enero de 2019

Fecha de publicación: 09/01/2019

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player
- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- .NET Framework
- ASP.NET
- Microsoft Exchange Server
- Microsoft Visual Studio

Descripción:

La publicación de actualizaciones de seguridad de Microsoft este mes consta de 48 vulnerabilidades, 8 clasificadas como críticas y 40 como importantes, siendo el resto de las publicadas de severidad media o baja.

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 a las siguientes:

- Revelación de información.
- Denegación de servicio.
- Ejecución remota de código.
- Escalado de privilegios.
- Suplantación (spoofing).

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

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 09/01/2019

Importancia: Alta

Recursos afectados:

- Productos Intel wireless con tecnologías anteriores a 20.90.0.7
  - Intel® Dual Band Wireless-AC 3160
  - Intel® Dual Band Wireless-AC 7260
  - Intel® Dual Band Wireless-N 7260
  - Intel® Wireless-N 7260
  - Intel® Dual Band Wireless-AC 7260 for Desktop
  - Intel® Dual Band Wireless-AC 7265 (Rev. C)
  - Intel® Dual Band Wireless-N 7265 (Rev. C)

    - Intel® Wireless-N 7265 (Rev. C)
    - Intel® Dual Band Wireless-AC 3165
    - Intel® Dual Band Wireless-AC 7265 (Rev. D)
    - Intel® Dual Band Wireless-N 7265 (Rev. D)
    - Intel® Wireless-N 7265 (Rev. D)
    - Intel® Dual Band Wireless-AC 3168
    - Intel® Tri-Band Wireless-AC 17265
    - Intel® Dual Band Wireless-AC 8260
    - Intel® Tri-Band Wireless-AC 18260
    - Intel® Dual Band Wireless-AC 8265
    - Intel® Dual Band Wireless-AC 8265 Desktop Kit
    - Intel® Tri-Band Wireless-AC 18265
    - Intel® Wireless-AC 9560
    - Intel® Wireless-AC 9461
    - Intel® Wireless-AC 9462
    - Intel® Wireless-AC 9260
- Intel® SSD Data Center Tool para Windows versiones anteriores a v3.0.17
- Intel® Optane™ SSD DC P4800X versiones anteriores E2010435
- Intel® System Support Utility para Windows versiones anteriores a 2.5.0.15
- Intel® SGX SDK para Windows versiones anteriores a 2.2.100
- Intel® SGX SDK para Linux versiones anteriores a 2.4.100
- Intel® SGX Platform Software para Windows versiones anteriores a 2.2.100
- Intel® SGX Platform Software para Linux versiones anteriores a 2.4.100

Descripción:

Intel ha publicado 5 avisos de seguridad en su centro de seguridad de productos que contienen 7 vulnerabilidades, 3 de criticidad alta y 4 de severidad media.

Solución:

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

Detalle:

Las vulnerabilidades de criticidad alta son las siguientes:

- Un usuario habilitado podría realizar una escalada de privilegios a través de un acceso local debido a:
    - Permisos de directorio incorrectos en ZeroConfig en el software Intel® PROSet/Wireless Wi-Fi. Se ha reservado el identificador CVE-2018-12177 para esta vulnerabilidad.
    - Comprobación insuficiente de la ruta en la utilidad de soporte del sistema Intel® para Windows. Se ha reservado el identificador CVE-2019-0088 para esta vulnerabilidad.
    - Verificación incorrecta de archivos en la rutina de instalación del software SDK de Intel® SGX para Windows. Se ha reservado el identificador CVE-2018-18098 para esta vulnerabilidad.

Se han reservado los identificadores CVE-2018-3703, CVE-2018-12166, CVE-2018-12167 y asignado el identificador CVE-2018-12155 para el resto de vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Omisión de sandbox en Pipeline y Script Security de Jenkins

Fecha de publicación: 09/01/2019

Importancia: Alta

Recursos afectados:

- Pipeline: Declarative Plugin versión 1.3.4 y anteriores.
- Pipeline: Groovy Plugin versión 2.61 y anteriores.
- Script Security Plugin versión 1.49 y anteriores.

Descripción:

Orange Tsai, de devcore, ha reportado una vulnerabilidad del tipo omisión del sandbox que afecta a Pipeline y a Script Security de Jenkins, que podría permitir a un atacante la ejecución arbitraria de código.

Solución:

Actualizar a las siguientes versiones:

- Pipeline: Declarative Plugin versión 1.3.4.1
- Pipeline: Groovy Plugin versión 2.61.1
- Script Security Plugin versión 1.50

Detalle:

- Una vulnerabilidad del tipo omisión del sandbox en Pipeline y en Script Security, podría permitir a un atacante con permiso Overall/Read o que sea capaz de controlar el contenido de la biblioteca compartida de Jenkinsfile o Pieline en SCM, pasar por alto la protección de la sandbox y ejectuar código arbitrario en el maestro de Jenkins.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de enero de

2019

Fecha de publicación: 09/01/2019

Importancia: Crítica

Recursos afectados:

- SAP Cloud Connector, versiones anteriores a 2.11.3
- SAP Landscape Management, versiones VCM 3.0
- SAP BW/4HANA, versión 1.0 (SP08)
- SAP Financial Consolidation Cube Designer, versiones BOBJ_EADES 8.0, 10.1
- SAP Commerce (ex. SAP Hybris Commerce), versiones anteriores a 6.7
- SAP Work Manager, versiones Agentry_SDK 7.0, 7.1
- SAP CRM WebClient UI, versiones SAPSCORE 1.12; S4FND 1.02; WEBCUIF 7.31, 7.46, 7.47, 7.48, 8.0, 8.01
- SAP Business Objects Mobile for Android, versiones anteriores a 6.3.5
- SAP Gateway of ABAP Application Server, versiones SAP_GWFND 7.5, 7.51, 7.52, 7.53; SAP_BASIS 7.5
- SAP Enterprise Financial Services, versiones SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; EA-FINSERV 1.10, 2.0, 5.0, 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0; Bank/CFM 4.63_20

Descripción:

SAP ha publicado varias actualizaciones de seguridad de diferentes productos en su comunicado mensual.

Solución:

Visitar el portal de soporte de SAP e instalar las actualizaciones o los parches necesarios, según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 11 notas de seguridad, siendo 2 de ellas de severidad crítica, 1 alta y 8 de criticidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de falta de verificación de autorización.
- 3 vulnerabilidades de cross-site scripting.
- 3 vulnerabilidades de revelación de información.
- 2 vulnerabilidades de denegación de servicio de redirección de URL.
- 1 vulnerabilidad de otro tipo.

Las notas de seguridad calificadas como críticas se refieren a:

- Dos vulnerabilidades en SAP Cloud Connector podrían permitir a un atacante leer, modificar o eliminar información sensible y acceder a funciones administrativas que requiere privilegios de administrador, debido a una falta de verificación de autorización. También podría permitir la inyección de código, provocando la ejecución de comandos no autorizados, acceso o revelación de información sensible o en denegación de servicio.
- Una vulnerabilidad en SAP Landscape Management podría permitir que un atacante obtenga las credenciales de un usuario con privilegios elevados.

En cuanto a la etiquetada con severidad alta, se trata de una vulnerabilidad del tipo falta de verificación de autorización.

Etiquetas: Actualización, SAP, Vulnerabilidad

Denegación de servicio en Email Security Appliance de Cisco

Fecha de publicación: 10/01/2019

Importancia: Crítica

Recursos afectados:

- Cisco AsyncOS Software para ESA Major Release
  - Versiones anteriores a 9.0,
  - Versión 9.x y 10.x
  - Versión 11.0.x y anteriores.
  - Versión 11.1.x y anteriores.

Descripción:

Cisco ha publicado dos vulnerabilidades que afectan a su producto Email Security Appliance (ESA), una de severidad crítica y otra alta. La explotación exitosa de alguna de estas vulnerabilidades puede derivar en una denegación de servicio (Dos).

Solución:

Cisco recomienda migrar/actualizar en función de la versión de su producto

- Versiones anteriores a 9.0 migrar a 11.0.2-044
- Versiones 9.x y 10.x migrar a 11.0.2-044
- Versiones 11.0.x actualizar a 11.0.2-044
- Versiones 11.1.x actualizar a 11.1.2-023 o a 11.1.1-037

Detalle:

- La explotación exitosa de alguna de estas dos vulnerabilidades podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) originada por:
  - Una validación de entrada incorrecta en la función de descifrado y verificación de las extensiones de correo electrónico, permitiendo corromper la memoria del sistema del dispositivo afectado. Se ha reservado el identificador CVE-2018-15453

para esta vulnerabilidad.
    - Un filtrado inadecuado de los mensajes de correo electrónico que contienen URLs de listas blancas, que permitiría al atacante elevar el uso de la CPU al 100%. Se ha reservado el identificador CVE-2018-15460 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Juniper

Fecha de publicación: 10/01/2019

Importancia: Crítica

Recursos afectados:

- Junos OS versiones 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2 en plataformas MX Series con configuración vlan dinámica.
- Junos OS 12.1X46 versiones anteriores a 12.1X46-D77 en plataformas SRX Series;
- Junos OS 12.3 versiones anteriores a 12.3R12-S10;
- Junos OS 12.3X48 versiones anteriores a 12.3X48-D70 en plataformas SRX Series;
- Junos OS 14.1X53 versiones anteriores a 14.1X53-D47 en plataformas EX2200/VC, EX3200, EX3300/VC, EX4200, EX4300, EX4550/VC, EX4600, EX6200, EX8200/VC (XRE), QFX3500, QFX3600, QFX5100;
- Junos OS 15.1 versiones anteriores a 15.1R3;
- Junos OS 15.1F versiones anteriores a 15.1F3;
- Junos OS 15.1X49 versiones anteriores a 15.1X49-D140 en plataformas SRX Series;
- Junos OS 15.1X53 versiones anteriores a 15.1X53-D59 en plataformas EX2300/EX3400.
- Junos OS versiones anteriores a 15.1 en plataformas vMX Series.
- Junos OS 14.1X53 versiones anteriores a 14.1X53-D47 en plataformas EX y QFX Virtual Chassis.
- Junos OS 15.1 versiones anteriores a 15.1R7-S3 en todas Virtual Chassis.
- Junos OS 15.1X53 versiones anteriores a 15.1X53-D50 en plataformas EX y QFX Virtual Chassis.
- Junos OS 12.1X46, 12.3X48, 15.1X49 en plataformas SRX Series.
- Junos OS 12.1X46, 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1.
- Junos OS 17.2X75, 17.4, 18.1, 18.2 en plataformas QFX y PTX Series.
- Juniper ATP en versiones 5.0.3 y 5.0.4

Descripción:

Juniper ha publicado 8 avisos de seguridad que contienen 13 vulnerabilidades, 5 de ellas de severidad crítica y 8 de importancia alta.

Solución:

- Visitar el apartado "Referencias" para obtener información detallada en función del producto afectado.

Detalle:

Las vulnerabilidades de severidad crítica son las siguientes:

- El software de la serie vMX utiliza un número de secuencia de identificación IP predecible. Esto hace que tanto el sistema como los clientes que se conectan a través del dispositivo sean susceptibles a una familia de ataques que se basan en el uso de números de secuencia de IP ID predecibles como método de ataque. Se ha reservado el identificador CVE-2019-0007 para esta vulnerabilidad.
- Un determinado paquete HTTP podría desencadenar una vulnerabilidad de desferencia de puntero de función no inicializada en el gestor del motor de redireccionamiento de paquetes (fxpc) de todos los dispositivos de las series EX, QFX y MX, en una configuración de Virtual Chassis. Esto podría provocar un fallo del demonio fxpc o permitir a un atacante la ejecución remota del código. Se ha reservado el identificador CVE-2019-0006 para esta vulnerabilidad.
- En Juniper ATP:
    - Web Collector utiliza credenciales embebidas. Se ha reservado el identificador CVE-2019-0020 para esta vulnerabilidad.
    - Dos credenciales embebidas que comparten la misma contraseña le dan al atacante la capacidad de tomar el control de cualquier instalación del software. Se ha reservado el identificador CVE-2019-0022 para esta vulnerabilidad.
    - Las credenciales de Splunk se registran en un archivo legible por usuarios locales autenticados. Usando estas credenciales, un atacante podría acceder al servidor Splunk. Se ha reservado el identificador CVE-2019-0029 para esta vulnerabilidad.

Para el resto de vulnerabilidades de severidad alta se han reservado los identificadores CVE-2019-0001, CVE-2019-0003, CVE-2019-0010, CVE-2019-0012, CVE-2019-0014, CVE-2017-11610, CVE-2019-0021, CVE-2019-0004.

Etiquetas: Actualización, Sistema Operativo, Vulnerabilidad

Vulnerabilidad de cadena de formato en FortiOS de FortiGuard

Fecha de publicación: 14/01/2019

Importancia: Alta

Recursos afectados:

- FortiOS versiones 5.6.0 y anteriores.

Descripción:

FortiGuard ha publicado una vulnerabilidad de cadena de formato en su sistema operativo FortiOS que podría permitir a un atacante la corrupción de memoria.

Solución:

- Actualizar a la versión FortiOS 5.6.1 o superior.

Detalle:

- Una vulnerabilidad de cadena de formato en el manejo del nombre de usuario SSH al conectarse a FortiOS versiones 5.6.0 y anteriores, puede permitir a un atacante provocar la corrupción de la memoria. Se ha reservado el identificador CVE-2018-1352 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en IBM Security Identity Manager

Fecha de publicación: 14/01/2019

Importancia: Crítica

Recursos afectados:

- IBM Security Identity Manager desde la versión 6.0.0 hasta 6.0.0.20.

Descripción:

IBM ha detectado múltiples vulnerabilidades en IBM Security Identity Manager (ISIM), que podrían permitir a un atacante comprometer cuentas de usuarios debido al uso de contraseñas débiles, subida o transferencia de archivos maliciosos o cross-site scripting (XSS).

Solución:

- IBM recomienda actualizar a la versión 6.0.0-ISS-SIM-FP0021.

Detalle:

- La vulnerabilidad de severidad crítica podría permitir a un atacante cargar archivos maliciosos que serían procesados automáticamente en el entorno del sistema. Se ha reservado el identificador CVE-2018-1969 para esta vulnerabilidad.

El resto de vulnerabilidades son de criticidad media y se les ha reservado el identificador CVE-2018-1956 y CVE-2018-1967.

Etiquetas: Actualización, IBM, Vulnerabilidad

Actualizaciones críticas en Oracle (Enero 2019)

Fecha de publicación: 16/01/2019

Importancia: Crítica

Recursos afectados:

- Enterprise Manager Base Platform, versiones 12.1.0.5, 13.2, 13.3
- Enterprise Manager for Virtualization, versiones 13.2.2, 13.2.3, 13.3.1
- Enterprise Manager Ops Center, versiones 12.2.2, 12.3.3
- Hyperion BI , versión 11.1.2.4
- Java Advanced Management Console, versión 2.12
- JD Edwards EnterpriseOne Tools, versión 9.2
- JD Edwards World Security, versiones A9.3, A9.3.1, A9.4
- MySQL Connectors, versiones 2.1.8 y anteriores, 8.0.13 y anteriores
- MySQL Enterprise Monitor, versiones 4.0.7 y anteriores, 8.0.13 y anteriores
- MySQL Server, versiones 5.6.42 y anteriores, 5.7.24 y anteriores, 8.0.13 y anteriores
- MySQL Workbench, versiones 8.0.13 y anteriores
- 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, versiones 6.2.0.0, 6.2.1.0, 6.2.2.0, 6.2.3.0, 6.2.3.1
- Oracle API Gateway, versión 11.1.2.4.0
- Oracle Application Testing Suite, versiones 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1
- Oracle Argus Safety, versiones 8.1, 8.2
- Oracle Banking Platform, versiones 2.5.0, 2.6.0, 2.6.1, 2.6.2
- Oracle Business Process Management Suite, versiones 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle Communications Billing and Revenue Management, versiones 7.5, 12.0
- Oracle Communications Converged Application Server, versiones anteriores a 7.0.0.1
- Oracle Communications Converged Application Server - Service Controller, versión 6.1
- Oracle Communications Diameter Signaling Router (DSR), versiones anteriores a 8.3
- Oracle Communications Online Mediation Controller, versión 6.1
- Oracle Communications Performance Intelligence Center (PIC) Software, versiones anteriores a 10.2.1
- Oracle Communications Policy Management, versiones anteriores a 12.5
- Oracle Communications Service Broker, versión 6.0
- Oracle Communications Services Gatekeeper, versiones anteriores a 6.1.0.4.0
- Oracle Communications Session Border Controller, versiones SCz7.4.0, SCz7.4.1, SCz8.0.0, SCz8.1.0
- Oracle Communications Unified Inventory Management, versiones anteriores a 7.4.0
- Oracle Communications Unified Session Manager, versión SCz7.3.5
- Oracle Communications WebRTC Session Controller, versiones anteriores a 7.2
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c
- 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, 12.2.8
- Oracle Endeca Server, versión 7.7.0
- Oracle Enterprise Communications Broker, versiones PCz2.1, PCz2.2, PCz3.0
- Oracle Enterprise Repository, versión 12.1.3.0.0
- Oracle Enterprise Session Border Controller, versiones ECz7.4.0, ECz7.5.0, ECz8.0.0, ECz8.1.0
- Oracle Financial Services Analytical Applications Infrastructure, versiones 7.3.3, 7.3.5, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6, 8.0.7
- Oracle FLEXCUBE Direct Banking, versión 12.0.2
- Oracle FLEXCUBE Investor Servicing, versiones 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0
- Oracle Fusion Middleware MapViewer, versión 12.2.1.3.0

- Oracle GoldenGate Application Adapters, versión 12.3.2.1.1
- Oracle Health Sciences Information Manager, versión 3.0
- Oracle Healthcare Foundation, versiones 7.1, 7.2
- Oracle Healthcare Master Person Index, versiones 3.0, 4.0
- Oracle Hospitality Cruise Fleet Management, versión 9.0.10
- Oracle Hospitality Cruise Shipboard Property Management System, versión 8.0.8
- Oracle Hospitality Reporting and Analytics, versión 9.1.0
- Oracle Hospitality Simphony, versión 2.10
- Oracle HTTP Server, versión 12.2.1.3
- Oracle Insurance Calculation Engine, versión 10.2
- Oracle Insurance Insbridge Rating and Underwriting, versiones 5.2, 5.4, 5.5
- Oracle Insurance Policy Administration J2EE, versiones 10.0, 10.2
- Oracle Insurance Rules Palette, versiones 10.0, 10.2
- Oracle Java SE, versiones 7u201, 8u192, 11.0.1
- Oracle Java SE Embedded, versión 8u191
- Oracle Managed File Transfer, versiones 12.2.1.3.0, 19.1.0.0.0
- Oracle Outside In Technology, versiones 8.5.3, 8.5.4
- Oracle Reports Developer, versión 12.2.1.3
- Oracle Retail Back Office, versiones 13.3, 13.4, 14.0, 14.1
- Oracle Retail Central Office, versiones 13.3, 13.4, 14.0, 14.1
- Oracle Retail Convenience and Fuel POS Software, versión 2.8.1
- Oracle Retail Customer Insights, versiones 15.0, 16.0
- Oracle Retail Integration Bus, versión 17.0
- Oracle Retail Merchandising System, versión 14.1
- Oracle Retail Returns Management, versiones 13.3, 13.4, 14.0, 14.1
- Oracle Retail Sales Audit, versión 15.0
- Oracle Retail Service Backbone, versiones 13.1, 13.2, 14.0, 14.1, 15.0, 16.0
- Oracle Retail Workforce Management Software, versiones 1.60.9, 1.64.0
- Oracle Retail Xstore Payment, versión 3.3
- Oracle Secure Global Desktop (SGD), versión 5.4
- Oracle Service Architecture Leveraging Tuxedo, versiones 12.1.3.0.0, 12.2.2.0.0
- Oracle SOA Suite, versiones 12.1.3.0.0, 12.2.1.3.0
- Oracle Solaris, versiones 10, 11
- Oracle Transportation Management, versiones 6.3.7, 6.4.1, 6.4.2, 6.4.3
- Oracle Utilities Framework, versión 4.3.0.1-4.3.0.4
- Oracle Utilities Network Management System, versiones 1.12.0.3, 2.3.0.0, 2.3.0.1, 2.3.0.2
- Oracle VM VirtualBox, versiones anteriores a 5.2.24, anteriores a 6.0.2
- Oracle Web Cache, versión 11.1.1.9.0
- Oracle WebCenter Portal, versiones 11.1.1.9.0, 12.2.1.3.0
- Oracle WebCenter Sites, versión 11.1.1.8.0
- Oracle WebLogic Server, versiones 10.3.6.0, 12.1.3.0, 12.2.1.3
- OSS Support Tools, versiones anteriores a 19.1
- PeopleSoft Enterprise CC Common Application Objects, versión 9.2
- PeopleSoft Enterprise CS Campus Community, versiones 9.0, 9.2
- PeopleSoft Enterprise HCM eProfile Manager Desktop, versión 9.2
- PeopleSoft Enterprise PeopleTools, versiones 8.55, 8.56, 8.57
- PeopleSoft Enterprise SCM eProcurement, versión 9.2
- Primavera P6 Enterprise Project Portfolio Management, versiones 8.4, 15.1, 15.2, 16.1, 16.2, 17.7-17.12, 18.8
- Primavera Unifier, versiones 16.1, 16.2, 17.1-17.12, 18.8
- Siebel Applications, versiones 18.10, 18.11
- Sun ZFS Storage Appliance Kit (AK), versiones anteriores a 8.8.2
- Tape Library ACSLS, versión 8.4

Descripción:

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

Solución:

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

Detalle:

- Esta actualización resuelve un total de 284 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.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Múltiples vulnerabilidades en productos de Microsoft

Fecha de publicación: 16/01/2019

Importancia: Alta

Recursos afectados:

- Team Foundation Server 2017 versión 3.1
- Team Foundation Server 2018 versiones 1.2 y 3.2
- Skype for Business Server 2015 CU 8

Descripción:

Microsoft ha corregido 3 vulnerabilidades fuera de ciclo, que afectaban a varios de sus productos.

Solución:

- Actualizar el sistema afectado a través de los parches automáticos distribuidos por Microsoft.

Detalle:

Las vulnerabilidades de severidad alta son las siguientes:

- Una vulnerabilidad de suplantación de identidad, cuando un servidor de Skype for Business Server no valida correctamente una solicitud especialmente diseñada, podría permitir a un atacante autenticado enviar dicha solicitud y ejectuar *scripts*. Se ha reservado el identificador CVE-2019-0624 para esta vulnerabilidad.
- Una vulnerabilidad de *Cross-site Scripting* (XSS), cuando Team Foundation Server no valida correctamente la información proporcionada por el usuario, podría permitir a un atacante autenticado enviar un *payload* especialmente diseñado, y ejecutar *scripts*, que le permitirían leer contenido no autorizado, ejecutar código malicioso y suplantar la identidad de la víctima. Se ha reservado el identificador CVE-2019-0646 para esta vulnerabilidad.

Para la vulnerabilidad de severidad media se ha reservado el identificador CVE-2019-0647.

Etiquetas: Actualización, Microsoft, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.2

Fecha de publicación: 16/01/2019

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones desde la 2.5.0 hasta la 3.9.2

Descripción:

Joomla! ha publicado una nueva versión que soluciona cuatro vulnerabilidades en el núcleo, todas ellas de criticidad baja.

Solución:

- Actualizar a la versión 3.9.2 disponible en su página web.

Detalle:

- Un escape inadecuado en *mod_banners* deriva en una vulnerabilidad XSS persistente. Se ha asignado el identificador CVE-2019-6264 para esta vulnerabilidad.
- Un escape inadecuado en *com_contact* deriva en una vulnerabilidad XSS persistente. Se ha asignado el identificador CVE-2019-6261 para esta vulnerabilidad.
- Las comprobaciones inadecuadas en la opción de configuración *Global Configuration Text Filter* permiten un XSS persistente. Se ha asignado el identificador CVE-2019-6263 para esta vulnerabilidad.
- Las comprobaciones inadecuadas en la opción de configuración *Global Configuration helpurl* permiten un XSS persistente. Se ha asignado el identificador CVE-2019-6262 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Gestión inadecuada de cookie en Jenkins

Fecha de publicación: 17/01/2019

Importancia: Alta

Recursos afectados:

- Jenkins Weekly, versiones 2.159 y anteriores.
- Jenkins LTS, versiones 2.150.1 y anteriores.

Descripción:

Dos vulnerabilidades en Jenkins, una de criticidad alta y otra media, debidas a una incorrecta gestión de la cookie "Remeber me", permitirían a un atacante acceder al sistema de forma persistente o la imposibilidad de invalidar sesiones activas o reiniciar Jenkins.

Solución:

Desde Jenkins recomiendan actualizar a las siguientes versiones:

- Jenkins Weekly versión 2.160
- Jenkins LTS versión 2.150.2

Detalle:

- La vulnerabilidad de criticidad alta permitiría a usuarios con permisos *Overall/RunScripts* generar una cookie "Remember me" que no expiraría nunca. Esto daría acceso a un atacante a una instancia de Jenkins, mientras exista el correspondiente usuario en el dominio de seguridad, además de que le permitiría acceder al sistema de manera persistente.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en el núcleo de Drupal

Fecha de publicación: 17/01/2019

Importancia: Crítica

Recursos afectados:

- Drupal versiones 7.x, 8.5.x y 8.6.x

Descripción:

El equipo de seguridad de Drupal ha publicado tres actualizaciones que corrigen múltiples vulnerabilidades en las versiones 7 y 8.

Solución:

- Actualizar a Drupal 7.62, 8.5.9 o 8.6.6 en función de la versión utilizada.

Las versiones de Drupal 8 anteriores a la 8.5.x están al final de su vida útil y no reciben cobertura de seguridad.

Detalle:

Las principales vulnerabilidades corregidas con estas actualizaciones son:

- El núcleo de Drupal utiliza la biblioteca PEAR Archive_Tar de terceros. Esta biblioteca ha publicado una actualización de seguridad que afecta a algunas configuraciones de Drupal. Se ha asignado el identificador CVE-2018-1000888 para esta vulnerabilidad.
- Una vulnerabilidad de ejecución de código remoto en el envoltorio integrado de *phar stream* de PHP, cuando se realizan operaciones de archivo en un *phar:// URI* no confiable, podría afectar a algunos códigos de Drupal (core, contrib y custom) que estén realizando operaciones de ficheros con entradas de usuario con validación incorrecta. Esta vulnerabilidad se ve mitigada por el hecho de que tales rutas de código normalmente requieren acceso con permisos de administrador o una configuración atípica.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

---

Vulnerabilidad en archivos .VCF de Microsoft Windows

Fecha de publicación: 23/01/2019

Importancia: Alta

Recursos afectados:

- Microsoft Windows

Descripción:

John Page (hyp3rlinx) ha descubierto una vulnerabilidad que permite al atacante la ejecución remota de código arbitrario en instalaciones vulnerables de Microsoft Windows, siendo necesaria la interacción del usuario para explotarla, ya que debe visitar una página maliciosa o abrir un archivo malicioso.

Solución:

- ZDI se ha puesto en contacto con Microsoft, pero han declarado que no abordarán este problema mediante una actualización de seguridad mensual, si no que el equipo solucionará esta cuestión en una futura versión de Windows.

Detalle:

- Esta vulnerabilidad afecta específicamente al procesamiento de los archivos de contactos de Windows (.VCF), debido a que modificando la información de un archivo de ese tipo se consigue que Windows muestre un hipervínculo malicioso. La interfaz de usuario no proporciona una indicación suficiente de la amenaza, y el atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario actual.

Etiquetas: 0day, Microsoft, Sistema Operativo, Vulnerabilidad

---

Vulnerabilidad de DoS en Apache HTTP Server

Fecha de publicación: 24/01/2019

Importancia: Alta

Recursos afectados:

- Apache HTTP Server versión 2.4.37 que tiene habilitado el módulo *mod_ssl* al usar OpenSSL 1.1.1 o posterior.

Descripción:

Una vulnerabilidad en el módulo *mod_ssl* de Apache HTTP Server permitiría que un atacante remoto no autenticado genere una condición de denegación de servicio (DoS) en el sistema objetivo.

Solución:

- Apache ha publicado la versión 2.4.38 de Apache HTTP Server para corregir esta vulnerabilidad.

Detalle:

- Esta vulnerabilidad se origina debido al manejo inadecuado de los intentos de renegociación por parte del software afectado cuando se utiliza OpenSSL 1.1.1 o posterior. Un atacante podría explotar esta vulnerabilidad enviando una solicitud con información maliciosa a un sistema objetivo, causando que el módulo *mod_ssl* entre en un bucle y no responda, provocando una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-0190 para esta vulnerabilidad.

Etiquetas: Apache, OpenSSL, Vulnerabilidad

Multiples vulnerabilidades en productos Cisco

Fecha de publicación: 24/01/2019

Importancia: Crítica

Recursos afectados:

- Cisco SD-WAN, versiones anteriores a 18.4.0 para los 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 Webex Business Suite WBS32 sites, todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión WBS32.15.33.
- Cisco Webex Business Suite WBS33 sites, todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión WBS33.6.1 y WBS 33.7.0.
- Cisco Webex Meetings Online, todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión 1.3.40.
- Cisco Webex Meetings Server, todas las versiones de Webex Network Recording Player anteriores a la versión 2.8MR3 SecurityPatch1 o 3.0MR2 SecurityPatch2.
- Cisco Webex Teams, versiones anteriores a 3.0.10260.
- Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers, con versiones desde 1.4.2.15 hasta 1.4.2.19.
- Connected Grid Network Management System, versiones anteriores a 3.0 de IoT-FND.
- Cisco Firepower Threat Defense Software, versión 6.3.0 cuando se ejecuta en las plataformas Firepower 4100 o Firepower 9300 Series.
- Cisco Identity Services Engine (ISE), versiones anteriores a 2.4 patch 1.

Descripción:

Cisco ha publicado 12 vulnerabilidades en varios de sus productos, siendo 1 de severidad crítica y 11 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 vulnerabilidad de severidad crítica es la siguiente:

- Una verificación incorrecta de los límites por parte del *vContainer* permitiría a un atacante remoto autenticado provocar una condición de denegación de servicio o ejecutar código arbitrario como usuario *root.* Se ha reservado el identificador CVE-2019-1651 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los identificadores: CVE-2019-1636, CVE-2019-1637, CVE-2019-1638, CVE-2019-1639, CVE-2019-1640, CVE-2019-1641, CVE-2019-1647, CVE-2019-1648, CVE-2019-1650, CVE-2019-1646, CVE-2019-1652, CVE-2019-1653, CVE-2019-1644, CVE-2019-1669 y CVE-2018-15459.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

Vulnerabilidad TLS Padding Oracle en productos Citrix

Fecha de publicación: 24/01/2019

Importancia: Alta

Recursos afectados:

Se ven afectadas las plataformas que no se encuentran en la siguiente lista y que ejecutan las siguientes versiones de Citrix ADC y NetScaler Gateway, incluidas las instancias de Citrix ADC en plataformas SDX que utilizan aceleración de hardware mediante una función virtual asignada (VF):

- Citrix ADC y NetScaler Gateway versión 12.1 anterior a la build 50.31
- Citrix ADC and NetScaler Gateway versión 12.0 anterior a la build 60.9
- Citrix ADC and NetScaler Gateway versión 11.1 anterior a la build 60.14
- Citrix ADC and NetScaler Gateway versión 11.0 anterior a la build 72.17
- Citrix ADC and NetScaler Gateway versión 10.5 anterior a la build 69.5

Las siguientes plataformas no se ven afectadas y no requieren la actualización del firmware:

- MPX 5900 series
- MPX/SDX 8900 series
- MPX/SDX 15000-50G
- MPX/SDX 26000-50S series
- MPX/SDX 26000-100G series
- MPX/SDX 26000 series
- VPX

Descripción:

Se ha identificado una vulnerabilidad en las plataformas Citrix Application Delivery Controller (ADC), formalmente conocido como NetScaler ADC, y NetScaler Gateway que podría permitir a un atacante explotar el dispositivo para descifrar el tráfico TLS.

Solución:

- Los dispositivos Citrix ADC y NetScaler Gateway que han desactivado las suites de cifrado basadas en CBC no se ven afectados por esta vulnerabilidad. Citrix también recomienda priorizar los cifrados basados en GCM.
- Citrix recomienda que los clientes afectados apliquen la mitigación adecuada o actualicen todos sus dispositivos vulnerables (Citrix ADC y NetScaler Gateway) a una versión del firmware del dispositivo que contenga una solución para este problema lo antes posible.

Detalle:

- La aceleración de hardware utilizada por las plataformas Citrix ADC y NetScaler Gateway podría permitir a un atacante explotar el dispositivo para descifrar el tráfico TLS. Esta vulnerabilidad no permite directamente a un atacante obtener la clave privada de TLS. Se ha reservado el identificador CVE-2019-6485 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en el gestor de paquetes APT

Fecha de publicación: 24/01/2019

Importancia: Alta

Recursos afectados:

- Gestor de paquetes APT, versiones anteriores a la 1.4.9

Descripción:

El investigador de seguridad Max Justicz ha descubierto una vulnerabilidad que permite la ejecución remota de código en la utilidad *apt-get* del gestor de paquetes APT, usada por distribuciones basadas en Debian.

Solución:

- Se podría evitar este tipo de ataque utilizando repositorios HTTPS por parte de APT, para ello es necesario instalar el paquete *apt-transport-https.*
- Actualizar, con la mayor brevedad posible, a la versión 1.4.9 de APT.

Para evitar que la vulnerabilidad sea explotada al realizar estas acciones, si el paquete se redirige de forma predeterminada, será necesario elegir diferentes réplicas o descargar el paquete directamente. Las siguientes instrucciones para Debian y Ubuntu indican cómo hacerlo correctamente.

Detalle:

- Los redireccionamientos HTTP de APT ayudan a las máquinas Linux a encontrar automáticamente el servidor espejo adecuado para descargar paquetes de software cuando otros no están disponibles, devolviendo una respuesta con la ubicación del siguiente servidor desde donde el cliente debe solicitar el paquete si el primer servidor falla de alguna manera. Esto puede permitir que un atacante, en un escenario de MitM (*Man in the Middle*), pueda inyectar contenido malicioso en los paquetes descargados por APT y engañar así al sistema para que instale paquetes alterados. Se ha reservado el identificador CVE-2019-3462 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Ubuntu, Vulnerabilidad

Actualización de seguridad de servidores DNS

Fecha de publicación: 25/01/2019

Importancia: Crítica

Recursos afectados:

- Para operadores de resolución DNS, se ven afectadas las versiones anteriores de los siguientes *resolvers* de DNS:
  - BIND 9.13.3 (desarrollo) y 9.14.0 (producción).
  - PowerDNS Recursor 4.2.0
  - Unbound 1.9.0
- Para operadores de servidores DNS, se puede comprobar si el dominio se ve afectado mediante el formulario de prueba.
- Si desea obtener un resultado detallado del test, puede utilizar la herramienta *ednscomp* (también se encuentra disponible su código fuente), cuyos resultados pueden ser:
  - *OK:* el dominio no está afectado.
  - *Compatible:* el dominio tiene algunos problemas, pero no se verá afectado el *DNS Flag Day*.
  - *High latency:* el dominio sufrirá de *timeouts* al tratar de resolverlo.
  - *Dead:* el dominio no funcionará.
  - Además, la herramienta *ednscomp* cuenta con dos modos:
    - *Permissive:* el modo para la situación anterior a *DNS Flag Day*.
    - *Strict:* después del *DNS Flag Day*.
- También es posible la comprobación de la compatibilidad de EDNS realizando las siguientes pruebas mediante el comando DIG. Más información en el siguiente enlace:
  - *dig norec noedns soa zone @server*
  - *dig norec edns=0 soa zone @server*
  - *dig norec edns=100 noednsneg soa zone @server*
  - *dig norec ednsopt=100 soa zone @server*
  - *dig norec ednsflags=0x80 soa zone @server*
  - *dig norec dnssec soa zone @server*

- *dig norec dnssec bufsize=512 ignore dnskey zone @server*
- *dig norec edns=100 noednsneg ednsopt=100 soa zone @server*

Descripción:

El 01/02/2019, los cuatro principales proveedores de software para DNS recursivos (Bind, Unbound, PowerDNS y Knot), realizarán un lanzamiento conjunto de nuevas versiones de sus sistemas con una característica en común: el fin de parches provisionales históricos que permitían ciertas prácticas inadecaudas del estándar en los servidores DNS autoritativos. Con este cambio, los *resolvers*, cuyos servidores de nombre incumplan el estándar EDNS, poco a poco comenzarán a fallar al resolver dominios.

Solución:

El administrador de los servidores de nombres afectados por estos cambios puede mitigar estas incompatibilidades cambiando la configuración del/de los servidor/es de nombres autorizado/s y posteriormente actualizando su software de DNS a las últimas versiones estables que se adhieran a los estándares. Una vez actualizado, deberá volver a realizar la prueba; si continúa fallando, deberá de verificar la configuración de su firewall para que no descarte paquetes DNS con extensiones EDNS, incluidas las extensiones desconocidas.

Además, es recomendable:

- Aplicar los parches de seguridad del fabricante o proveedor, si procede. La información relevante de algunos fabricantes se puede encontrar aquí:
  - Akamai
  - BlueCat
  - F5 BIG-IP
  - Juniper: las versiones anteriores de Juniper SRX eliminarán los paquetes EDNS de forma predeterminada. La solución es deshabilitar la manipulación de DNS a través del comando ***# set security alg dns doctoring none***. Actualizar a las últimas versiones para el soporte de EDNS.
  - Infoblox
- Cumplimiento de EDNS, en particular, lo recomendado es implementar *cookies* DNS (RFC 7873) que requieren que las opciones de EDNS desconocidas sean manejadas correctamente por todos los servidores.
- Implementación de DNSSEC (*Domain Name System Security Extensions*).
- Revisar periódicamente los servidores DNS.
- Considerar migrar a una solución basada en dispositivo.
- Considerar migrar a una solución DNS comprobando previamente la problemática de EDNS.
- Corregir, en la medida de lo posible, cualquier problema identificado, solicitando asistencia técnica a sus proveedores de software (o preguntando a su empresa de alojamiento de dominios) cuando sea necesario.
- Revisar con la herramienta ednscomp.
  - Tal vez solo se necesite actualizar el software de su servidor DNS a la versión más actual.
  - Verificar que todos los balanceadores de carga o *proxies* DNS de su empresa sean compatibles y estén correctamente configurados.
  - Revisar si los *firewalls* o enrutadores que intentan inspeccionar paquetes DNS están correctamente actualizados.

Detalle:

Los mecanismos de extensión para DNS especificados en 1999 y actualizados en 2013 para establecer las 'reglas de tránsito' que respondieran a las consultas con opciones o indicadores de EDNS, continúan sufriendo fallos e incompatibilidades en algunas de sus implementaciones. Los desarrolladores de software de DNS han intentado resolver estos problemas de interoperabilidad en el protocolo, especialmente en su extensión EDNS (estándar RFC 6891), mediante varias soluciones alternativas para comportamientos no estándar que se aplicarán a el 1 de febrero del 2019.

A partir de esa fecha, los dominios de servidores DNS que no cumplan con el estándar, no funcionarán, y la presencia online de los dominios que resuelven esos servidores, se degradará o desaparecerá lentamente a medida que los ISP y otras organizaciones actualicen sus resoluciones. Además, cuando actualicen sus resoluciones de DNS internas a versiones que no implementan soluciones alternativas, es posible que algunos sitios y servidores de correo electrónico dejen de estar disponibles.

Otros problemas que pueden surgir a causa de estas soluciones son:

- DNS autoritativos que bloquean respuestas. Las respuestas excesivamente lentas a las consultas de DNS y la dificultad de implementar nuevas funciones de protocolo DNS. Algunas de estas nuevas características (por ejemplo, las *cookies* de DNS) ayudarían a reducir los ataques DDoS basados en el abuso del protocolo DNS.
- Malas implementaciones de DNS que no siguen los estándares.
- Los servidores DNS que no responden en absoluto a las consultas de EDNS serán tratados como no accesibles.
- Los servidores DNS autoritativo bloquean las respuestas, o no contestan, o responden con el paquete incorrecto. En general, las malas implementaciones de DNS no siguen los estándares. (DNS *resolvers* tienen que esperar a *timeout* y reintentar con TCP o sin EDNS).
- *Firewalls* mal implementados o malas políticas que bloquean tráfico que sigue los estándares.

Etiquetas: Actualización, Comunicaciones, DNS

Múltiples vulnerabilidades en phpMyAdmin

Fecha de publicación: 28/01/2019

Importancia: Crítica

Recursos afectados:

Las siguientes versiones de phpMyAdmin se han visto afectadas:

- Desde 4.0 hasta 4.8.4.
- Desde 4.5.0 hasta 4.8.4.

Impacto:

El equipo de phpMyAdmin ha publicado la versión 4.8.5, que contiene varias correcciones de seguridad importantes.

Solución:

- Se recomienda actualizar a la versión 4.8.5 o superior de phpMyAdmin.

Detalle:

- En las versiones que van desde la 4.0 hasta la 4.8.4, cuando la configuración *AllowArbitraryServer* se le asigna el valor *true* en un servidor MySQL no autorizado, un atacante podría leer cualquier archivo del servidor al que el usuario tuviera acceso. Se ha asignado el identificador 2019-6799 para esta vulnerabilidad.
- En las versiones que van desde la 4.5.0 hasta la 4.8.4, un atacante podría usar un nombre de usuario especialmente diseñado para iniciar un ataque de inyección SQL a través de la función *designer.* Se ha asignado el identificador CVE-2019-6798 para esta vulnerabilidad.

Etiquetas: Actualización, PHP, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 29/01/2019

Importancia: Alta

Recursos afectados:

- Active Directory Plugin, versión 2.10 y anteriores.
- Blue Ocean Plugin, versión 1.10.1 y anteriores.
- Config File Provider Plugin, versión 3.4.1 y anteriores.
- Git Plugin, versión 3.9.1 y anteriores.
- GitHub Authentication Plugin, versión 0.29 y anteriores.
- Groovy Plugin, versión 2.0 y anteriores.
- Job Import Plugin, versión 2.1 y anteriores.
- Job Import Plugin, versión 3.0 y anteriores.
- Kanboard Plugin, versión 1.5.10 y anteriores.
- Monitoring Plugin, versión 1.74.0 y anteriores.
- OpenId Connect Authentication Plugin, versión 1.4 y anteriores.
- Script Security Plugin, versión 1.50 y anteriores.
- Token Macro Plugin, versión 2.5 y anteriores.
- Warnings Plugin, versión 5.0.0 y anteriores.
- Warnings Next Generation Plugin, versión 2.1.1 y anteriores.
- Warnings Next Generation Plugin, versión 1.0.1 y anteriores.

Descripción:

Jenkins ha publicado 20 vulnerabilidades que afectan a varios de sus productos, siendo 6 de ellas de severidad alta y las demás categorizadas como medias o bajas.

Solución:

- Active Directory Plugin, actualizar a la versión 2.11
- Blue Ocean Plugin, actualizar a la versión 1.10.2
- Config File Provider Plugin, actualizar a la versión 3.5
- Git Plugin, actualizar a la versión 3.9.2
- GitHub Authentication Plugin, actualizar a la versión 0.31
- Groovy Plugin, actualizar a la versión 2.1
- Job Import Plugin, actualizar a la versión 3.0
- Job Import Plugin, actualizar a la versión 3.1
- Kanboard Plugin, actualizar a la versión 1.5.11
- Monitoring Plugin, actualizar a la versión 1.75.0
- OpenId Connect Authentication Plugin, actualizar a la versión 1.5
- Script Security Plugin, actualizar a la versión 1.51
- Token Macro Plugin, actualizar a la versión 2.6
- Warnings Plugin, actualizar a la versión 5.0.1
- Warnings Next Generation Plugin, actualizar a la versión 2.1.2
- Warnings Next Generation Plugin, actualizar a la versión 2.0.0

Detalle:

Las vulnerabilidades de severidad alta son:

- Validación de certificados incorrecta con StartTLS en Active Directory Plugin, se ha asignado el identificador SECURITY-859.
- *XML External Entity* (XXE), se ha asignado el identificador SECURITY-905 (1).
- Sandbox Bypass en Script Security Plugin, se ha asignado el identificador SECURITY-1292.
- Sandbox Bypass en Groovy Plugin, se ha asignado el identificador SECURITY-1293.
- Sandbox Bypass vía CSRF en Warnings Plugin, se ha asignado el identificador SECURITY-1295 (1).
- Sandbox Bypass vía CSRF en Warnings Plugin Next Generation Plugin, se ha asignado el identificador SECURITY-1295 (2).

Para el resto de vulnerabilidades se han asignado los identificadores: SECURITY-602, SECURITY-797, SECURITY-818, SECURITY-886, SECURITY-905 (2), SECURITY-1095, SECURITY-1102, SECURITY-1153, SECURITY-1154, SECURITY-1201, SECURITY-1204, SECURITY-1253, SECURITY-1271 y SECURITY-1302.

Etiquetas: Actualización, Vulnerabilidad

Microsoft Exchange 2013 y posteriores, vulnerables a ataques NTLM relay

Fecha de publicación: 29/01/2019

Importancia: Alta

Recursos afectados:

- Microsoft Exchange 2013 y posteriores.

Descripción:

Microsoft Exchange 2013 y posteriores no pueden establecer indicadores de firma y sello en el tráfico de autenticación NTLM, lo que podría permitir a un atacante remoto obtener los privilegios del servidor de Exchange con respecto al objeto Dominio en Active Directory.

Solución:

Actualmente no se conoce solución práctica para esta vulnerabilidad.

Considerar las siguientes soluciones alternativas:

- Si no se utilizan las suscripciones push/pull de EWS, puede bloquear la llamada a PushSubscription API que desencadena este ataque, para ello, ejecute los siguientes comandos desde una ventana de Shell de administración de Exchange:
  - New-ThrottlingPolicy -Nombre NoEWSS Subscription -ThrottlingPolicyScope Organization -EwsMaxSubscriptions 0
  - Restart-WebAppPool -Nombre MSExchangeServicesAppPool
- Eliminar los privilegios de Exchange en el objeto de dominio (esta solucion ha sido recomendada por el descubridor de la vulnerabilidad. Es recomendable probar cualquier solución en su entorno de pruebas para asegurarse de que funcionan correctamente):
  - Este script de PowerShell puede ejecutarse tanto en el sistema Exchange Server como en el Domain Controller. Por defecto, buscará entradas de control de acceso vulnerables en el directorio activo actual. Cuando se ejecuta con privilegios de administrador de dominio y la marca *-Fix*, este script eliminará la capacidad de Exchange para escribir en el objeto de dominio.
  - Tenga en cuenta que si encuentra un error al no reconocer *Get-ADDomainController*, necesitará instalar e importar el módulo *ActiveDirectory PowerShell* y, finalmente, ejecutar *Fix-DomainObjectDACL.ps1*:
    - *Import-Module ServerManager*
    - *Add-WindowsFeature RSAT-AD-PowerShell*
    - *Import-Module ActiveDirectory*
    - *.Fix-DomainObjectDACL.ps1*
  - Si el script informa de que se ha encontrado un ACE defectuoso, ejecute:
    - *.Fix-DomainObjectDACL.ps1 -Fix*
  - PowerShell puede configurarse para bloquear la ejecución de archivos.ps1 proporcionados por el usuario. Si este es el caso, primero busque su política de ejecución de PowerShell actual:
    - *Get-ExecutionPolicy*
  - Permita temporalmente la ejecución del script Fix-DomainObjectDACL.ps1 mediante la ejecución:
    - *Set-ExecutionPolicy unrestricted*
  - Una vez que haya terminado de ejecutar el script Fix-DomainObjectDACL.ps1, vuelva a establecer la política en el valor original tal y como indica Get-ExecutionPolicy:
    - *Set-ExecutionPolicy [POLICY]*
- Eliminar los privilegios innecesarios que Exchange tiene sobre el objeto Dominio.
- Habilitar la firma LDAP y habilitar el enlace de canales LDAP para evitar la retransmisión a LDAP y LDAPS respectivamente.
- Bloquear los servidores Exchange para que no puedan realizar conexiones a estaciones de trabajo en puertos arbitrarios.
- Habilitar la protección ampliada para la autenticación en los endpoints de Exchange en IIS (pero no en los endpoints de Exchange, esto haría que Exchange dejase de funcionar). Esto verificará los parámetros de enlace de canales en la autenticación NTLM, que vincula la autenticación NTLM a una conexión TLS y evita la retransmisión a los servicios web de Exchange.
- Eliminar la clave de registro que hace posible la retransmisión al servidor de Exchange, como se explica en la mitigación de Microsoft para CVE-2018-8518.
- Establecer el inicio de sesión SMB en servidores Exchange (y preferiblemente en todos los demás servidores y estaciones de trabajo del dominio) para evitar ataques de retransmisión entre protocolos a SMB.

Detalle:

- Microsoft Exchange admite una API llamada Exchange Web Services (EWS). Una de las funciones de la API de EWS, llamada PushSubscription, puede utilizarse para que el servidor Exchange se conecte a un sitio web arbitrario, estas conexiones intentarán negociar con el servidor web arbitrario mediante la autenticación NTLM. A partir de Microsoft Exchange 2013, la autenticación NTLM sobre HTTP falla al establecer los indicadores de firma y sello NTLM, lo que hace que sea vulnerable a los ataques de retransmisión NTLM.
- Microsoft Exchange está configurado de forma predeterminada con privilegios con respecto al objeto Dominio en Active Directory. Debido a que el grupo Exchange Windows Permissions tiene acceso WriteDacl al objeto Dominio, los privilegios de servidor de Exchange obtenidos mediante esta vulnerabilidad se podrían utilizar para obtener privilegios de administrador en el dominio que contiene el servidor de Exchange vulnerable.
- Un atacante que posea credenciales para un buzón de correo de Exchange y con la capacidad de comunicarse tanto con un servidor de Microsoft Exchange como con un controlador de dominio de Windows, puede obtener privilegios de administrador de dominio. Un atacante que no se encuentre en posesión de la contraseña también puede realizar un ataque de retransmisión de SMB a HTTP, siempre y cuando se encuentren en el mismo segmento de red que el servidor de Exchange.

Etiquetas: Correo electrónico, Microsoft, Vulnerabilidad

Vulnerabilidad en BIG-IP TMUI de F5

Fecha de publicación: 30/01/2019

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
  - Desde 13.0.0 hasta 13.1.1
  - Desde 12.1.0 hasta 12.1.3
  - Desde 11.6.0 hasta 11.6.3

Descripción:

BIG-IP ha publicado una vulnerabilidad de tipo *cross-site scripting* reflejado (*reflected XSS*) en una página no revelada de la Interfaz de Usuario de Gestión de Tráfico (*Traffic Management User Interface*, TMUI) de BIG-IP, también conocida como la utilidad de Configuración BIG-IP.

Solución:

Si se está ejecutando una versión vulnerable, se puede eliminar esta vulnerabilidad actualizando a una de las siguientes versiones desde su centro de descarga de *software*:

- 14.1.0 y 14.0.0.3
- 13.1.1.4
- 12.1.4
- 11.6.3.3

Detalle:

- Para realizar el ataque, el usuario debe visitar una URL especialmente diseñada que incluya el nombre de *host* de destino específico. Si el *exploit* tiene éxito, el atacante ejecuta JavaScript en el contexto del usuario conectado actualmente. En el caso de un administrador con acceso a *Advanced Shell* (*bash*), se puede aprovechar la explotación exitosa de esta vulnerabilidad para comprometer completamente el sistema BIG-IP a través de una ejecución remota de código. Se ha reservado el identificador CVE-2019-6589 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en coTURN

Fecha de publicación: 30/01/2019

Importancia: Crítica

Recursos afectados:

- coTURN versiones 4.5.0.9 y anteriores.

Descripción:

Se han detectado tres vulnerabilidades en servidores coTURN, una de severidad crítica, una de criticidad media y otra aún reservada, por lo que se desconoce su criticidad, que podrían permitir a un atacante acceder a la cuenta de administración del servidor.

Solución:

- Actualizar a la versión 4.5.1.0.

Detalle:

- Un atacante podría acceder al portal de administración del servidor mediante una inyección SQL con un nombre de usuario especialmente diseñado en la web de acceso de coTURN. Se ha asignado el identificador CVE-2018-4056 para esta vulnerabilidad de severidad crítica.
- Una configuración por defecto insegura en el servidor coTURN, podría permitir a un atacante emplear una cuenta de administración telnet que se encuentra sin credenciales para acceder al servidor con permisos de administrador. Se ha asignado el identificador CVE-2017-4059 para esta vulnerabilidad de severidad media.
- A la vulnerabilidad que no ha sido publicada aún, se le ha reservado el identificador CVE-2018-4058.

Etiquetas: Actualización, Vulnerabilidad