Boletín de diciembre de 2018

Avisos Técnicos

Vulnerabilidad en TLS de Mbed

Fecha de publicación: 04/12/2018

Importancia: Alta

Recursos afectados:

- Todas las versiones de Mbed TLS.

Descripción:

La vulnerabilidad de criticidad alta podría permitir a un atacante local sin privilegios recuperar el texto plano del descifrado RSA que se utiliza en las suites de cifrado RSA-sin-(EC)DH(E).

Solución:

- Actualizar a una de las versiones más recientes de Mbed TLS, incluyendo 2.14.1, 2.7.8 o 2.1.17 o posteriores.
- Las versiones actualizadas de Mbed TLS siguen siendo vulnerables a una de las fugas si el tamaño de la clave RSA no es múltiplo del tamaño de palabra de la máquina, por lo que se recomienda que se utilicen tamaños de clave que sean múltiplos de 64 bits.

Detalle:

- La vulnerabilidad podría permitir a un atacante ejecutar código y recuperar el texto sin formato a través de un *Bleichenbacher oracle*. En particular, afecta a las conexiones (D)TLS que utilizan descifrado RSA, donde el atacante podría descifrar la conexión mediante un ataque de recuperación de texto en el servidor o interceptar la conexión mediante un ataque man-in-the-middle sobre el contenido. Se ha reservado el CVE-2018-19608 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 05/12/2018

Importancia: Alta

Recursos afectados:

- IBM Campaign versiones 9.1.0 y 9.1.2
- IBM QRadar SIEM desde la versión 7.2.0 hasta la 7.2.8 Patch 13 y desde la versión 7.3.0 hasta la 7.3.1 Patch 6

Descripción:

IBM ha reportado varias vulnerabilidades en sus productos Campaign y QRadar SIEM que podrían permitir la escalada de privilegios, la divulgación de información o la denegación del servicio.

Solución:

- Para IBM Campaign versión 9.1.0 actualizar a la versión 9.1.0.13
- Para IBM Campaign versión 9.1.2 actualizar a la vesión 9.1.2.7
- Para IBM QRadar SIEM desde la versión 7.2.0 hasta la 7.2.8 Patch 13 actualizar a la versión QRadar / QRM / QVM / QRIF / QNI 7.2.8 Patch 14
- Para IBM QRadar SIEM desde la versión 7.3.0 hasta la 7.3.1 Patch 6, actualizar a la versión QRadar / QRM / QVM / QRIF / QNI 7.3.1 Patch 7

Detalle:

- IBM Campaign podría permitir a un usuario local obtener privilegios de administrador debido a que la aplicación no valida los

permisos de acceso. Se ha reservado el identificador CVE-2018-1941 para esta vulnerabilidad.
- IBM QRadar es vulnerable a un ataque de *XML External Entity Injection* (XXE) al procesar datos XML que podría permitir a un atacante remoto exponer información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2018-1730 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 07/12/2018

Importancia: Crítica

Recursos afectados:

- Jenkins Weekly versión 2.153 y anteriores.
- Jenkins LTS versión 2.138.3 y anteriores.

Descripción:

Jenkins ha publicado 4 vulnerabilidades en varios productos, siendo 1 de severidad crítica y 3 de severidad media.

Solución:

- Jenkins Weekly actualizar a la versión 2.154
- Jenkins LTS actualizar a la versión 2.138.4 o a 2.150.1

Detalle:

A continuación se detalla únicamente la vulnerabilidad de severidad crítica, que tiene asignado el identificador SECURITY-595.

- Para el manejo de peticiones HTTP, Jenkins utiliza el framework web S*tapler* el cual emplea el acceso reflexivo a elementos de código que coinciden con sus convenciones de nomenclatura, dado que estas coinciden estrechamente con los patrones de código comunes en Java, el acceso a URLs diseñadas podría invocar métodos que nunca tuvieron la intención de ser invocados de esta manera. Esto podría derivar en que los usuarios:
  - No autenticados podrían invalidar todas las sesiones cuando ejecutan Jenkins con el servidor *Winstone-Jetty* integrado.
  - Con permiso *Overall/Read* podrían crear nuevos objetos de usuario en la memoria.
  - Con permiso *Overall/Read* podrían iniciar manualmente las ejecuciones de implementaciones de *AsyncPeriodicWork* que de otro modo se ejecutarían periódicamente.

Para las demás vulnerabilidades, Jenkins ha asignado los siguientes identificadores: SECURITY-904, SECURITY-1072 y SECURITY-1193

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Cloud Kubernetes Service y en Marketing Platform de IBM

Fecha de publicación: 07/12/2018

Importancia: Crítica

Recursos afectados:

- IBM Cloud Kubernetes Service versiones desde la 1.12.0 hasta la 1.12.2, desde la 1.11.0 hasta la 1.11.4, desde la 1.10.0 hasta la 1.10.10 y desde la 1.5 hasta la 1.9
- IBM Marketing Platform versiones 9.1.0, 9.1.2 y 10.1

Descripción:

IBM ha publicado varias vulnerabilidades que podrían permitir el acceso no autorizado o la escalada de privilegios en Kubernetes API Server y la divulgación de información o el consumo de memoria en IBM Marketing Platform.

Solución:

- Para IBM Clud Kubernetes Service, compruebe la versión de su *clúster* mediante el comando *clusters de ibmcloud ks* y verifique lo siguiente:
  - Las versiones 1.10 y posteriores han sido actualizadas sin necesidad de intervención por parte de los usuarios.
  - Las versiones 1.12.3, 1.11.5 o 1.10.11, no se ven afectadas por la vulnerabilidad.
  - Si el *clúster* se encuentra en las versiones 1.10, 1.11 o 1.12 y no se ha actualizado automáticamente, contacte con el servicio IBM Cloud Support para obtener ayuda.
  - Las versiones 1.8 y 1.9 deberán actualizar a las versiones 1.10, 1.11 o 1.12.
  - Las versión 1.7 deben actualizarse previamente a la versión 1.9 y posteriormente a la 1.10, 1.11 o 1.12.
  - La versión 1.5 no es posible actualizar.
- Para IBM Marketing Platform:
  - Versión 9.1.0 actualizar a la 9.1.0.13
  - Versión 9.1.2 actualizar a la 9.1.2.6-IBM_MP-IF01
  - Versión 10.1 actualizar a la 10.1.0.1

Detalle:

- Un manejo inadecuado de las solicitudes en el servidor API de Kubernetes pordría permitir a un atacante remoto, mediante una solicitud de proxy especialmente diseñada enviada directamente al *backend*, establecer una conexión y crear servicios gestionados e implementar código malicioso con privilegios elevados, Se ha asignado el código CVE-2018-1002105 para esta vulnerabilidad de severidad crítica.
- IBM Marketing Platform es vulnerable a un ataque de XML *External Entity Injection* (XXE) al procesar datos XML. Un atacante remoto podría exponer información sensible o consumir recursos de memoria. Se han reservado los códigos CVE-2018-1920 y

CVE-2018-1424 para estas vulnerabilidades de severidad alta.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad en varios productos de F5

Fecha de publicación: 07/12/2018

Importancia: Crítica

Recursos afectados:

- BIG-IP (APM) versiones:
  - 14.0.0
  - 13.0.0 - 13.1.1
  - 12.1.0 - 12.1.3
- BIG-IP APM Clients versión desde la 7.1.5 hasta la 7.1.7, ambas incluidas.
- BIG-IP Edge Client versión desde la 7101 hasta la 7150, ambas incluidas.

Descripción:

La explotación exitosa de esta vulnerabilidad podría permitir que un usuario local sin privilegios vea información sensible, manipule ciertos datos o que adquiera privilegios de superusuario en el *host* del cliente local.

Solución:

- BIG-IP (APM) en las versiones afectadas, por el momento no hay solución.
- BIG-IP APM Clients actualizar a la versión 7.1.7.2
- BIG-IP Edge Client en las versiones afectadas, por el momento no hay solución.

Detalle:

- El componente *svpn* del cliente F5 BIG-IP APM, se ejecuta como un proceso privilegiado y podría permitir que un usuario sin privilegios obtenga la propiedad de los archivos con atributos de *root* en el *host* del cliente local en condiciones de carrera. Se ha asignado el identificador CVE-2018-15332 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de diciembre 2018

Fecha de publicación: 12/12/2018

Importancia: Crítica

Recursos afectados:

- SAP Business Client Versión 6.5
- SAP Commerce (SAP Hybris Commerce), versiones 6.2, 6.3, 6.4, 6.5, 6.6, 6.7
- SAP Basis (?AS ABAP of SAP NetWeaver? 700 a 750, para 750 posteriormente entregadas como ?ABAP Platform?) versiones 7.00 a 7.02, 7.10 a 7.30, 7.31, 7.40, 7.50 a 7.53
- SAP NetWeaver, versiones - ServerCore (7.11, 7.20, 7.30, 7.31, 7.40, 7.50)
- SAP NetWeaver (Application Server Java Library), versiones 7.20, 7.30, 7.31 y 7.50
- SAP NetWeaver AS Java, versiones ServerCore (7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50)
- SAP ABAP Change and Transport System (CTS), versiones SAP KERNEL 32 NUC, SAP KERNEL 32 Unicode, SAP KERNEL 64 NUC, SAP KERNEL 64 Unicode 7.21, 7.21EXT, 7.22 y 7.22EXT; SAP KERNEL 7.21, 7.22, 7.45, 7.49, 7.53, 7.73, 7.74
- SAP Marketing, versiones UICUAN (1.20, 1.30, 1.40), SAPSCORE (1.13, 1.14)
- SAP_BASIS, versiones 6.40, 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40
- SAP Business One Service Layer, versión B1_ON_HANA (9.2, 9.3)
- SAP Mobile Secure for Android, versión 6.60.19942.0 SP28 1711
- SAP HANA, versiones 1.0, 2.0

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 2 de ellas de severidad crítica, 3 altas y 6 de criticidad media y 1 de severidad baja.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de falta de verificación de autorización.
- 3 vulnerabilidades de cross-site scripting.
- 1 vulnerabilidades de divulgación de información.
- 1 vulnerabilidad de incorrecta validación de XML.
- 1 vulnerabilidad de cross-frame scripting.
- 4 vulnerabilidades de otro tipo.

Las clasificadas como críticas son las siguientes:

- Una vulnerabilidad en SAP Business Client versión 6.5 podría permitir a un atacante ejecutar código arbitrario dentro de una *sandbox* a través de una página de HTML previamente diseñada.
- Una vulnerabilidad cross-site scripting (XSS) en SAP Hybris Commerce, afecta al archivo *JavaScript webApplicationInjector.js* o a una copia de él cuando lo utilizan las tiendas.

Etiquetas: Actualización, SAP, Vulnerabilidad

Boletín de seguridad de Microsoft de diciembre de 2018

Fecha de publicación: 12/12/2018

Importancia: Crítica

Recursos afectados:

- Adobe Flash Player.
- Internet Explorer.
- Microsoft Edge.
- Microsoft Windows.
- Microsoft Office y Microsoft Office Services y Web Apps.
- ChakraCore.
- .NET Framework.
- Microsoft Dynamics NAV.
- Microsoft Exchange Server.
- Microsoft Visual Studio.
- Windows Azure Pack (WAP).

Descripción:

La publicación de actualizaciones de seguridad de Microsoft este mes consta de 39 vulnerabilidades, 9 clasificadas como críticas y 30 como importantes, siendo el resto 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.
- Escalada de privilegios.
- Suplantación (*spoofing*).
- Manipulación (*tampering*).

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

---

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 12/12/2018

Importancia: Alta

Recursos afectados:

- Intel® Solid State Drive Toolbox versiones anteriores a la 3.5.7
- Intel(R) VTune Amplifier 2018 Update 3 y anteriores.
- Intel® Parallel Studio anterior a Intel® System Studio 2019 Gold.
- Intel® System Defense Utility todas las versiones.
- Intel(R) QuickAssist Technology para Linux.

Descripción:

Intel ha publicado 5 avisos de seguridad en su centro de seguridad de productos de severidades: 1 alta, 3 medias y 1 baja.

Solución:

- Para Intel® Solid State Drive Toolbox:
  - Desinstalar la versión preexistente de Intel® Solid State Drive Toolbox.
  - Actualizar a la versión 3.5.7 o posterior.
- Para Intel(R) VTune Amplifier:
  - Actualizar a Intel® VTune Amplifier 2019 Update 1 o posterior.
- Para Intel® Parallel Studio:
  - Actualizar a la v2019 Update 1 or later.
- Para Intel® System Defense Utility:
  - Intel ha emitido un aviso de suspensión de productos para esta utilidad y recomienda a los usuarios que la desinstalen o dejen de usarla lo antes posible.
- Para Intel(R) QuickAssist Technology:
  - CVE-2018-12206: evalúe las notas de la versión, sección 3.1.4, para detectar posibles cambios en el entorno de implementación de la VM.
  - CVE-2018-18096: la funcionalidad se ha eliminado en R4.3 y se restablecerá en la versión R4.4 y posteriores.

Detalle:

- Los permisos incorrectos en Intel® Solid State Drive Toolbox anteriores a la versión 3.5.7 podrían permitir a un atacante autenticado habilitar la escalada de privilegios a través del acceso local. Se ha reservado el identificador CVE-2018-18097 para esta vulnerabilidad de severidad alta.

Los identificadores reservados para el resto de vulnerabilidades de severidad media y baja son: CVE-2018-18093, CVE-2018-3704, CVE-2018-3705 y CVE-2018-18096.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en WebSphere Application Server de IBM

Fecha de publicación: 12/12/2018

Importancia: Alta

Recursos afectados:

- IBM WebSphere Application, versiones 9.0, 8.5, 8.0 y 7.0

Descripción:

IBM ha publicado una vulnerabilidad de severidad alta que afecta a su producto WebSphere Application Server y que podría permitir la ejecución remota de código.

Solución:

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

- Para versiones desde la 9.0.0.0 hasta la 9.0.0.9 existen dos opciones:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PH04060.
  - Aplicar el *Fixpack* 9.0.0.10 o posterior (disponibilidad prevista 4Q2018).
- Para versiones desde la 8.5.0.0 hasta la 8.5.5.14 existen dos opciones:
  - Actualizar a los niveles mínimos de *Fixpack* requeridos por los IFIX y luego aplicar el *Interim Fix* PH04060.
  - Aplicar el *Fixpack* 8.5.5.15 o posterior (disponibilidad prevista 1Q2019).
- Para versiones desde la 8.0.0.0 hasta la 8.0.0.15:
  - Actualizar a la versión 8.0.0.15 y luego aplicar el *Interim Fix* PH04060.
- Para versiones desde la 7.0.0.0 hasta la 7.0.0.45:
  - Actualizar a la versión 7.0.0.45 y luego aplicar el *Interim Fix* PH04060.

Detalle:

- Una vulnerabilidad en IBM WebSphere Application Server podría permitir a un atacante remoto ejecutar código Java arbitrario a través de una clase de cliente administrativo con un objeto serializado de fuentes no confiables. Se ha asignado el identificador CVE-2018-1904 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en WordPress

Fecha de publicación: 13/12/2018

Importancia: Alta

Recursos afectados:

- WordPress versiones 5.0 y anteriores.

Descripción:

WordPress ha publicado una actualización de seguridad para corregir 7 vulnerabilidades descubiertas por diversos investigadores.

Solución:

- Actualizar WordPress a la versión 5.0.1 disponible en su centro de descargas.

Detalle:

WordPress ha publicado un total de 7 vulnerabilidades del tipo:

- Alteración de metadatos para eliminar archivos sin autorización.
- Creación de publicaciones no autorizadas con entrada específicamente diseñada.
- Inyección de objetos en PHP mediante la modificación de metadatos.
- *Cross-site scripting* en la edición de comentarios con privilegios elevados.
- *Cross-site scripting* en entradas URL especialmente diseñadas.
- Exposición de direcciones de email, y en casos raros contraseñas, generadas por defecto.
- *Cross-site scripting* en *host* alojados en Apache.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en phpMyAdmin

Fecha de publicación: 13/12/2018

Importancia: Alta

Recursos afectados:

Las siguientes versiones de phpMyAdmin se han visto afectadas:

- Desde 4.0 hasta 4.8.3
- Desde 4.7.0 hasta 4.7.6 y desde 4.8.0 hasta 4.8.3

Descripción:

El equipo de phpMyAdmin ha publicado la versión 4.8.4, que contiene varias correcciones de seguridad importantes.

Solución:

- Se recomienda actualizar a la versión 4.8.4 o superior de phpMyAdmin.

Detalle:

- Las versiones desde 4.0 hasta 4.8.3 incluyen un error de inclusión de archivos locales (*Local File Inclusion*, LFI) que podría permitir la lectura de archivos locales del servidor a un atacante remoto. Se ha asignado el identificador CVE-2018-19968 para esta vulnerabilidad. Además, para estas mismas versiones, se ha identificado otra vulnerabilidad de *Cross-site Scripting* (XSS) con la que un atacante puede inyectar código malicioso a través de un nombre de tabla/base de datos especialmente diseñado. Se ha asignado el identificador CVE-2018-19970 para esta vulnerabilidad.
- Para las versiones desde 4.7.0 hasta 4.7.6 y desde 4.8.0 hasta 4.8.3 se ha encontrado un fallo que podría permitir a un atacante realizar operaciones SQL malintencionadas mediante un ataque *Cross-site Request Forgery* (CSRF). Se ha asignado el identificador CVE-2018-19969 para esta vulnerabilidad.

Etiquetas: Actualización, PHP, Vulnerabilidad

Vulnerabilidad en Operational Decision Manager de IBM

Fecha de publicación: 13/12/2018

Importancia: Alta

Recursos afectados:

- IBM Operational Decision Manager versiones 8.6, 8.7, 8.8 y 8.9

Descripción:

IBM ha publicado una vulnerabilidad en su producto Operational Decision Manager que podría permitir a un atacante remoto exponer información sensible o consumir recursos de la memoria.

Solución:

Seleccione la siguiente solución provisional para actualizar la instalación de ODM en función de la versión de su producto:

Interim fix para APAR RS03231 y RS03192 disponibles desde IBM Fix Central:

- IBM Operational Decision Manager v8.6:
  - 8.6.0.3-WS-ODM_DS-IF035
- IBM Operational Decision Manager v8.7:
  - 8.7.1.2-WS-ODM_DS-IF079
- IBM Operational Decision Manager v8.8:
  - 8.8.1.3-WS-ODM_DS-IF090
- IBM Operational Decision Manager v8.9:
  - 8.9.2.1-WS-ODM_DS-IF004

Detalle:

- IBM Operational Decision Manager es vulnerable a un ataque de XML *External Entity Injection* (XXE) al procesar datos XML. Un atacante remoto podría explotar esta vulnerabilidad para exponer información sensible o consumir recursos de la memoria. Se ha reservado el identificador CVE-2018-1821 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 14/12/2018

Importancia: Alta

Recursos afectados:

- D3600 y D6000, versiones de firmware anteriores a 1.0.0.75
- D6100, versiones de firmware anteriores a 1.0.0.58
- D7800, versiones de firmware anteriores a 1.0.1.42
- D8500, versiones de firmware anteriores a 1.0.3.42

- EX3700 y EX3800, versiones de firmware anteriores a 1.0.0.70
- EX6000, versiones de firmware anteriores a 1.0.0.30
- EX6100, versiones de firmware anteriores a 1.0.2.24
- EX6120, versiones de firmware anteriores a 1.0.0.40
- EX6130, versiones de firmware anteriores a 1.0.0.22
- EX6150, versiones de firmware anteriores a 1.0.0.42
- EX6200, versiones de firmware anteriores a 1.0.3.88
- EX7000, versiones de firmware anteriores a 1.0.0.66
- EX6100v2 y EX6150v2, versiones de firmware anteriores a 1.0.1.70
- EX6200v2, versiones de firmware anteriores a 1.0.1.64
- EX6400 y EX7300, versiones de firmware anteriores a 1.0.2.136
- R6100, versiones de firmware anteriores a 1.0.1.16
- R6250, versiones de firmware anteriores a 1.0.4.26
- R6300-2CXNAS, versiones de firmware anteriores a 1.0.3.60
- R6300v2, versiones de firmware anteriores a 1.0.4.28
- R6400, versiones de firmware anteriores a 1.0.1.36
- R6400v2, versiones de firmware anteriores a 1.0.2.52
- R6700 y R6900, versiones de firmware anteriores a 1.0.1.46
- R7000, versiones de firmware anteriores a 1.0.9.28
- R7100LG, versiones de firmware anteriores a 1.0.0.46
- R7300, versiones de firmware anteriores a 1.0.0.68
- R7500, versiones de firmware anteriores a 1.0.0.110
- R7500v2, versiones de firmware anteriores a 1.0.3.36
- R7800, versiones de firmware anteriores a 1.0.2.32
- R7900, versiones de firmware anteriores a 1.0.2.10
- R8000, versiones de firmware anteriores a 1.0.4.18
- R8900 y R9000, versiones de firmware anteriores a 1.0.4.12
- R8300 y R8500, versiones de firmware anteriores a 1.0.2.122
- R6900P y R7000P, versiones de firmware anteriores a 1.3.1.44
- R7900P, y R8000P, versiones de firmware anteriores a 1.3.0.10
- WAC120, versiones de firmware anteriores a 2.1.7
- WAC505 y WAC510, versiones de firmware anteriores a 5.0.5.4
- WNAP320, WNAP210v2, WNDAP350, WNDAP360 y WNDAP660, versiones de firmware anteriores a 3.7.11.4
- WNDAP620, versiones de firmware anteriores a 2.1.7
- WND930, versiones de firmware anteriores a 2.1.5
- WN604, versiones de firmware anteriores a 3.3.10
- WN2500RPv2, versiones de firmware anteriores a 1.0.0.54
- WN3000RPv2 y WNR3500Lv2, versiones de firmware anteriores a 1.2.0.56
- WN3000RPv3, versiones de firmware anteriores a 1.0.2.52
- WNDR3700v4, versiones de firmware anteriores a 1.0.2.102
- WNDR4300, versiones de firmware anteriores a 1.0.2.104
- WNDR4300v2 y WNDR4500v3, versiones de firmware anteriores a 1.0.0.50
- WNR2000v5, versiones de firmware anteriores a 1.0.0.66
- ReadyNAS OS 6, versiones de firmware anteriores a 6.9.3
- SRR60 y SRS60, versiones de firmware anteriores a 2.2.1.210

Descripción:

Netgear ha publicado 22 vulnerabilidades, de las cuales 6 son de severidad alta.

Solución:

- Actualizar a la última versión de firmware disponible en su centro de descargas.

Detalle:

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

- Inyección de comandos antes de la autenticación.
- Inyección de comandos después de la autenticación.
- Cross-site request forgery.
- Cross-site scripting.
- Configuración incorrecta de la seguridad en puntos de acceso inalámbricos.
- Desbordamiento de pila antes de la autenticación.
- Desbordamiento de pila después de la autenticación.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en varios productos de F5

Fecha de publicación: 17/12/2018

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator)
  - Desde la versión 14.0.0 hasta la 14.1.0
  - Desde la versión 13.1.0 hasta la 13.1.1
- BIG-IQ Centralized Management
  - Desde la versión 6.0.0 hasta la 6.0.1
  - Desde la versión 5.2.0 hasta la 5.4.0

Descripción:

Un atacante remoto podría conectar un ordenador al puerto de depuración y ejecutar un JavaScript arbitrario.

Solución:

- Para BIG-IQ Centralized Management, desde la versión 6.0.0 hasta la 6.0.1, actualizar a la versión 6.1.0.
- Para los demás productos y versiones, por el momento no se han publicado actualizaciones, se puede consultar cómo mitigar esta

vulnerabilidad en la página de F5, publicada en la sección de *Referencias*.

Detalle:

- Una vulnerabilidad que afecta a Node.js (versiones anteriores a la 6.15.0), utilizado por el componente iRulesLX de F5, podría permitir que un atacante remoto se conecte al puerto 5858 utilizado para depurar en cualquier interfaz de forma predeterminada y ejecute JavaScript arbitrario. Se ha asignado el identificador CVE-2018-12120 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en vRealize Operations de VMWare

Fecha de publicación: 19/12/2018

Importancia: Alta

Recursos afectados:

- VMWare vRealize Operations (vROps) versiones:
  - 7.x
  - 6.7.x
  - 6.6.x

Descripción:

El investigador Alessandro Zanni, *pentester* de OVH, ha detectado una vulnerabilidad de escalada de privilegios locales.

Solución:

Reemplazar o aplicar el parche correspondiente en función de la versión afectada:

- vRealize Operations 7.0.0.11287810
- vRealize Operations 6.7.0.11286837
- vRealize Operations 6.6.1.11286876

Detalle:

- vROps contiene una vulnerabilidad de escalada de privilegios locales debido a unos permisos inadecuados de los *scripts* de soporte. El usuario *administrador* de la aplicación vROPS con acceso al terminal podría explotar este problema para elevar los privilegios de *root* en una máquina vROPS. Se ha asignado el identificador CVE-2018-6978 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en Cisco Adaptative Security Appliance (ASA)

Fecha de publicación: 20/12/2018

Importancia: Alta

Recursos afectados:

- Todos los productos Cisco que ejecuten el software ASA y tengan habilitado el acceso de administración web.

Descripción:

Cisco ha publicado una vulnerabilidad de escalada de privilegios en Cisco Adaptive Security Appliance (ASA).

Solución:

Cisco recomienda actualizar o cambiar de versión:

- Versiones anteriores a la 9.3, migrar a la versión 9.4.4.29
- Versión 9.4, actualizar a 9.4.4.29
- Versión 9.5, migrar a la versión 9.6.4.20
- Versión 9.6, actualizar a 9.6.4.20
- Versión 9.7, migrar a la versión 9.8.3.18
- Versión 9.8, actualizar a 9.8.3.18
- Versión 9.9, actualizar a 9.9.2.36
- Versión 9.10, actualizar a 9.10.1.7

El software está disponible desde su centro de descargas.

Detalle:

- Una validación incorrecta de los privilegios de los usuarios al utilizar la interfaz de administración web podría permitir a un atacante remoto autenticado pero sin privilegios realizar acciones privilegiadas utilizando esta interfaz. Se ha reservado el identificador CVE-2018-15465 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 20/12/2018

Importancia: Alta

Recursos afectados:

- IBM Domino, versiones desde 9.0.1 hasta 9.0.1 FP10 IF4 y desde 9.0 hasta 9.0 IF4
- IBM Notes, versiones desde 9.0.1 hasta 9.0.1 FP10 IF5 y desde 9.0 hasta 9.0 IF4
- IBM API Connect, versiones desde 2018.1 hasta 2018.4.1 y desde 5.0.0.0 hasta 5.0.8.4

Descripción:

IBM ha reportado varias vulnerabilidades en sus productos Domino, Notes y API Connect que podrían permitir escalada de privilegios, omisión de autenticación, inyección NoSQL y escalar permisos propios.

Solución:

- Para IBM Domino 9.0.1 FP10IF5, consultar esta nota técnica provisional .
- Para IBM Notes Standard 9.0.1 FP10IF6, descargar Fix Central ID Notes_901FP10IF6_W32_Standard.
- Para IBM Notes Basic 9.0.1 FP10IF6, descargar Fix Central ID Notes_901FP10IF6_W32_Basic.
- Para IBM API Connect, descargar las versiones 2018.4.1.1 o 5.0.8.5 según corresponda.

Detalle:

- IBM Notes y Domino (sólo en Windows) contienen una vulnerabilidad de escalada de privilegios. Al crear una línea de comandos enviada a través del IPC de memoria compartida, se puede engañar al servicio *Notes System Diagnostic* (NSD) para que ejecute un archivo *dll* malicioso elegido por el atacante. Se ha reservado el identificador CVE-2018-1771 para esta vulnerabilidad.
- IBM LoopBack podría permitir a un atacante eludir la autenticación si el modelo *AccessToken* se expone a través de una API REST, ya que es posible crear un *AccessToken* para cualquier usuario, siempre que conozca el ID de usuario y, por lo tanto, obtener acceso a los datos de los demás usuarios o a sus privilegios. Se ha reservado el identificador CVE-2018-1778 para esta vulnerabilidad.
- IBM API Connect se ve afectado por una inyección de NoSQL en el conector MongoDB para el framework LoopBack. Se ha reservado el identificador CVE-2018-1784 para esta vulnerabilidad.
- API Connect V5 permite a un usuario con acceso limitado al nivel de *API Administrator* darse acceso completo al nivel de *Administrator* a través de la funcionalidad de miembros. Se ha reservado el identificador CVE-2018-1973 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de corrupción de memoria en Internet Explorer de Microsoft

Fecha de publicación: 20/12/2018

Importancia: Alta

Recursos afectados:

- Internet Explorer 9, 10 y 11

Descripción:

Microsoft ha publicado un aviso fuera de ciclo sobre una vulnerabilidad de ejecución remota de código debido a un fallo en la gestión que realiza el motor de *scripting* a la hora de manejar los objetos de la memoria de Internet Explorer.

Solución:

- Microsoft por el momento no ha encontrado solución para esta vulnerabilidad.
- Como medida de mitigación Carnegie Mellon University ha publicado una serie de medidas de protección.

Detalle:

- La explotación exitosa de esta vulnerabilidad podría permitir a un atacante corromper la memoria, lo que podría derivar en la ejecución de código arbitrario en el contexto del usuario actual u obtener los mismos privilegios que dicho usuario. En caso de obtener privilegios de administrador, el atacante podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con privilegios de administrador. Se ha reservado el identificador CVE-2018-8653 para esta vulnerabilidad.

Etiquetas: Microsoft, Navegador, Vulnerabilidad

Vulnerabilidad de inserción de archivos en Kibana

Fecha de publicación: 21/12/2018

Importancia: Crítica

Recursos afectados:

- Kibana versiones anteriores a 6.4.3 y 5.6.13

Descripción:

Se ha publicado una vulnerabilidad en Kibana, en el proceso LFI (*Local File Inclusion*) que podría permitir la inserción de archivos a través de peticiones http.

Solución:

- Actualizar a la versión 6.5

Detalle:

- Un atacante a través del API de la consola de Kibana podría enviar una solicitud http que le permita ejecutar ficheros Java Script que se encuentren alojados en cualquier directorio del servidor en los que Kibana tenga permisos, lo que le permitiría obtener información y ejecutar comandos que le permitan incluir ficheros para hacerse con el control de la máquina. Se ha asignado el identificador CVE-2018-17246 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de WIBU-SYSTEMS

Fecha de publicación: 21/12/2018

Importancia: Crítica

Recursos afectados:

- WibuKey.sys, versión 6.40 (Build 2400)
- Administrador de servidores WibuKey Network, versión 6.40.2402.500

Descripción:

El investigador Marcin 'Icewall' Noga, de Cisco Talos, ha descubierto dos vulnerabilidades de divulgación de información de la memoria del *kernel* y de escalada de privilegios por corrupción de *pool* en el producto WibuKey.sys, y otra de ejecución remota de código en WibuKey Network.

Solución:

- Descargar la última versión de *WibuKey for Users* desde el centro de software.

Detalle:

- Una solicitud IRP especialmente diseñada puede hacer que el controlador devuelva la memoria no inicializada, lo que resulta en la revelación de información de la memoria del *kernel*. Se ha reservado el identificador CVE-2018-3989 para esta vulnerabilidad.
- Una petición IRP especialmente diseñada puede causar un desbordamiento de búfer, resultando en corrupción de la memoria del *kernel*. Se ha reservado el identificador CVE-2018-3990 para esta vulnerabilidad.
- Un paquete TCP especialmente diseñado puede causar desbordamiento de *heap* y permitir la ejecución remota de código a nivel de *kernel*. Se ha reservado el identificador CVE-2018-3991 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Fuga de credenciales Wi-Fi en routers Livebox de Orange

Fecha de publicación: 28/12/2018

Importancia: Crítica

Recursos afectados:

- Livebox Arcadyan ARV7519RW22-A-L T VR9 1.2

Descripción:

El investigador de seguridad Troy Mursch, de Bad Packets LLC, ha publicado una vulnerabilidad que podría permitir a un atacante remoto obtener la contraseña Wi-Fi y el SSID de la red interna de los routers Livebox 2.1.

Solución:

- El *firmware* del módem Orange Livebox Arcadyan ARV7519, versión 00.96.00.96.96.613E, ha sido parcheado contra este fallo.

Detalle:

- Una vulnerabilidad presente en los dispositivos Orange Livebox 00.96.320S podría permitir a un atacante remoto descubrir credenciales Wi-Fi a través de una petición GET de tipo */get_getnetworkconf.cgi* en el puerto 8080, consiguiendo un control total si la contraseña de administrador es igual a la contraseña Wi-Fi o si tiene el valor de administrador predeterminado. Se ha asignado el identificador CVE-2018-20377 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad