Boletín de abril de 2019

Avisos Técnicos

Múltiples vulnerabilidades en Security Privileged Identity Manager Appliance de IBM

Fecha de publicación: 01/04/2019

Importancia: Crítica

Recursos afectados:

- IBM Security Privileged Identity Manager versión 2.1.1

Descripción:

IBM ha publicado un boletín de seguridad que está compuesto por 48 vulnerabilidades, siendo una vulnerabilidad de severidad crítica, 16 de severidad alta y el resto medias o bajas.

Solución:

IBM ha publicado un parche que mitiga las vulnerabilidades, puede descargarse a través del siguiente enlace.

Detalle:

Las vulnerabilidades encontradas son del tipo:

- Escalada de privilegios.
- Cierre inesperado.
- Ejecución arbitraria de comandos.
- Ejecución arbitraria de código.
- Fallo de memoria.
- Generar una condición de denegación de servicio.
- Revelación de información
- Eludir restricciones de acceso.
- Modificar y/o inyectar cookies.

A la vulnerabilidad de severidad crítica se le ha asignado el identificador CVE-2017-16939, y para las de severidad alta, se les han asignado los identificadores CVE-2018-1087, CVE-2018-1068, CVE-2016-1181, CVE-2014-0114, CVE-2018-15688, CVE-2018-5391, CVE-2017-1000050, CVE-2018-0494, CVE-2018-1113, CVE-2018-8897, CVE-2015-5180, CVE-2017-15670, CVE-2017-18017 y CVE-2017-11368. Y se han reservado los identificadores CVE-2018-1640 y CVE-2018-1618 para vulnerabilidades de criticidad alta.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Apache HTTP Server

Fecha de publicación: 02/04/2019

Importancia: Alta

Recursos afectados:

- Apache HTTP Server, versiones 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1 y 2.4.0.

Descripción:

Apache ha publicado 6 vulnerabilidades, 3 de severidad alta y 3 de criticidad baja.

Solución:

- Actualizar a la versión 2.4.39.

Detalle:

Las vulnerabilidades de criticidad alta son:

- En Apache HTTP Server con MPM (*Módulos de MultiProcesamiento*) event, worker o prefork, el código que se ejecuta en procesos o subprocesos secundarios con pocos privilegios (incluyendo *scripts* ejecutado por un intérprete de *scripts*), podría permitir a un atacante ejecutar código arbitrario con los privilegios de *root* manipulando el marcador. Se ha reservado el identificador CVE-2019-0221 para esta vulnerabilidad.
- Una condición de secuencia en *mod_auth_digest* cuando se está ejecutando en un servidor de subprocesos, podría permitir a un usuario con credenciales válidas autenticarse usando otro nombre de usuario y omitiendo las restricciones de control de acceso. Se ha reservado el identificador CVE-2019-0217 para esta vulnerabilidad.
- Un error en *mod_ssl* al utilizar la verificación de certificados de cliente por ubicacion con TLSv1.3, podría permitir a un atacante que soporte la autenticación *Post-Handshake* eludir las restricciones de control de acceso. Se ha reservado el identificador CVE-2019-0215 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han reservado los identificadores CVE-2019-0197, CVE-2019-0196 y CVE-2019-0220.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades en Db2 de IBM

Fecha de publicación: 03/04/2019

Importancia: Alta

Recursos afectados:

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

Descripción:

Se han publicado dos vulnerabilidades de tipo *buffer overflow* en Db2 que podrían permitir a un atacante local ejecutar código arbitrario como *root*.

Solución:

- Aplicar el parche apropiado en función de la versión. Consultar las *Referencias*.

Detalle:

- IBM DB2 libdb2e.so.1 es vulnerable a un desbordamiento de búfer basado en una pila, causado por una comprobación incorrecta de los límites que podría permitir a un atacante ejecutar código arbitrario. Se ha reservado el identificador CVE-2018-1936 para esta vulnerabilidad.
- IBM DB2 para Linux, UNIX y Windows (incluyendo DB2 Connect Server) es vulnerable a un desbordamiento de búfer, que podría permitir a un atacante local autenticado ejecutar código arbitrario en el sistema como *root*. Se ha reservado el identificador CVE-2019-4014 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad en FortiOS

Fecha de publicación: 05/04/2019

Importancia: Alta

Recursos afectados:

- FortiOS versiones:
  - 6.0.2 y anteriores.
  - 5.6.7 y anteriores.
  - 5.4.10 y anteriores.

Descripción:

Un usuario autenticado y sin privilegios podría cambiar la configuración del enrutamiento.

Solución:

En función de la versión del producto afectado, actualizar a las versiones:

- 6.0.3 o superior.
- 5.6.8 o superior.
- 5.4.11 o superior.

Detalle:

- Un control externo de la vulnerabilidad del sistema en FortiOS podría permitir a un usuario autenticado cambiar los ajustes de enrutamiento del dispositivo mediante la conexión al componente ZebOS. Se ha reservado el identificador CVE-2018-13371 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Elevación de privilegios en Módulo Fibre Channel de 16 Gb HPE Virtual Connect SE para Synergy

Fecha de publicación: 08/04/2019

Importancia: Crítica

Recursos afectados:

- Módulo Fibre Channel de 16 Gb HPE Virtual Connect SE para Synergy con *firmware* 5.00.50

Descripción:

Una vulnerabilidad en el módulo Fibre Channel de 16 Gb HPE Virtual Connect SE para Synergy podría permitir la elevación no autorizada de privilegios local o remota.

Solución:

- Actualizar a la versión 5.51.01 del *firmware* incluida en la versión actualizada de HPE Synergy Custom SPP 2018.11.20190405 y en HPE Synergy Custom SPP 2019.03.20190401, ambas disponibles en la página de descarga HPE Synergy Software Release

Detalle:

- La vulnerabilidad podría permitir la elevación no autorizada de privilegios local o remota. Se ha reservado el identificador CVE-2018-7120 para esta vulnerabilidad.

Etiquetas: HP, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 08/04/2019

Importancia: Crítica

Recursos afectados:

- IBM QRadar SIEM 7.3.2 GA - 7.3.2 GA Interim Fix 1
- IBM API Connect versión 2018.1-2018.4.1.3

Descripción:

IBM ha publicado dos vulnerabilidades en dos de sus productos. La explotación exitosa de alguna de ellas podría permitir una evasión de la autenticación o un escalado de privilegios.

Solución:

- IBM QRadar SIEM actualizar a 7.3.2 GA - 7.3.2 GA Interim Fix 2
- IBM API Connect actualizar a la versión 2018.4.1.4 fixpack

Detalle:

- Una vulnerabilidad en IBM QRadar SIEM, podría permitir a un atacante eludir la autenticación, exponiendo alguna funcionalidad que podría derivar en la divulgación de información o en la modificación de la configuración de la aplicación. Se ha reservado el identificador CVE-2019-4210 para esta vulnerabilidad.
- Una vulnerabilidad en IBM API Connect's Developer Portal, podría permitir a un atacante el escalado de privilegios cuando se integra con un registro de usuario de OpenID Connect (OIDC). Se ha reservado el identificador CVE-2019-4155 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de abril de 2019

Fecha de publicación: 10/04/2019

Importancia: Crítica

Recursos afectados:

- Microsoft Windows
- Microsoft Edge
- Internet Explorer
- Azure
- Microsoft Exchange
- Team Foundation Server
- Open Enclave SDK
- ASP .NET

Descripción:

La publicación de actualizaciones de seguridad de Microsoft de este mes consta de 75 vulnerabilidades, 16 clasificadas como críticas y 59 como importantes.

Solución:

- Instalar la actualización de seguridad correspondiente. En la página de información de la instalación de las mismas actualizaciones,

se informa de los distintos métodos para llevarlas a cabo.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- escalada de privilegios,
- divulgación de información,
- ejecución remota de código,
- manipulación,
- suplantación,
- denegación de servicio.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Vulnerabilidad en la autenticación en ActiveMatrix BusinessWorks de TIBCO

Fecha de publicación: 10/04/2019

Importancia: Crítica

Recursos afectados:

- TIBCO ActiveMatrix BusinessWorks, versiones 6.4.2 y anteriores.

Descripción:

El componente HTTP Connector de BusinessWork contiene una vulnerabilidad que permite que un cliente HTTP malintencionado ejecute con éxito las solicitudes HTTP sin autenticarse cuando se utiliza la autenticación básica con XML.

Solución:

- Actualizar a versiones 6.5.0 o superiores.

Detalle:

- El componente HTTP Connector contiene una vulnerabilidad que permite que las solicitudes HTTP de usuarios no autenticados sean procesadas por BusinessWorks, incluso cuando se requiere la autenticación. Esto sólo es posible cuando la política de autenticación básica de HTTP se usa junto con XML. BusinessWorks podría utilizar credenciales de una solicitud HTTP anterior con fines de autorización. Se ha asignado el identificador CVE-2019-8990 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en Media SDK de Intel

Fecha de publicación: 10/04/2019

Importancia: Alta

Recursos afectados:

- Intel® Media SDK, versiones anteriores a 2018 R2.1

Descripción:

Intel ha descubierto una vulnerabilidad en su producto Intel® Media SDK que podría permitir una escalada de privilegios.

Solución:

- Intel recomienda actualizar el producto afectado a la versión 2018 R2.1 o superior desde su centro de descarga.

Detalle:

- La utilización de permisos de directorio incorrectos en el instalador del producto Intel(R) Media SDK, en versiones anteriores a 2018 R2.1, podría permitir que un usuario autenticado habilite la escalada de privilegios a través del acceso local. Se ha reservado el identificador CVE-2018-18094 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.5

Fecha de publicación: 10/04/2019

Importancia: Alta

Recursos afectados:

- Joomla! CMS, versiones desde 1.5.0 hasta 3.9.4

Descripción:

Joomla! ha publicado una nueva versión que soluciona tres vulnerabilidades en su núcleo, 1 de criticidad alta, 1 de criticidad media y otra de criticidad baja. Estas vulnerabilidades son del tipo violación del control de acceso,*Cross-site scripting (XSS)* y salto de directorio.

Solución:

- Actualizar a la versión 3.9.5.

Detalle:

- La vulnerabilidad de criticidad alta se corresponde con una violación de las listas de control de acceso (ACL). Un atacante sin autenticación, podría realizar peticiones no autorizadas al aprovechar una fallo en la comprobación de acceso en el endpoint *"refresh list of helpsites"* de *com_users*. Se ha reservado el identificador CVE-2019-10946 para esta vulnerabilidad.
- A la vulnerabilidad de criticidad media no se le ha asignado identificador, ya que se encuentra pendiente de anunciar.
- A la vulnerabilidad de criticidad baja se le ha reservado el identificador CVE-2019-10945.

Etiquetas: Actualización, CMS, Windows

Actualización de seguridad de SAP de abril de 2019

Fecha de publicación: 10/04/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5
- SAP Crystal Reports for Visual Studio, versión 2010
- AP NetWeaver (SLD Registration) y 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, KERNEL desde 7.21 hasta 7.22, 7.45 y 7.49
- SAP BASIS, versiones desde la 7.00 hasta la 7.02, desde 7.10 hasta la 7.30, 7.31, 7.40 y desde la 7.50 hasta la 7.53
- SAP NetWeaver Process Integration (Runtime Workbench y Messaging System), versiones desde la 7.10 hasta la 7.11 ambas incluidas, 7.31, 7.40 y 7.50
- SAP HANA, versiones 1.0 y 2.0
- AP Enterprise Financial Services, versiones SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; EA-FINSERV 1.10, 2.0, 5.0, 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0 y Bank/CFM 4.63_20

Descripción:

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

Solución:

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

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 6 notas de seguridad y 3 actualizaciones, siendo 1 de ellas de severidad crítica, 2 alta y 6 de criticidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de falta de verificación de autorización.
- 3 vulnerabilidades de revelación de información.
- 2 vulnerabilidades *XML External Entity* (XXE).
- 2 vulnerabilidades de otro tipo.

La actualización de seguridad calificada como crítica se refiere a:

- El navegador Chromium que incluye Sap Business Client contiene múltiples vulnerabilidades que SAP ha solucionado en esta actualización.

Las notas de seguridad calificadas como altas se refieren a:

- SAP Crystal Reports contiene una vulnerabilidad de revelación de información, un atacante podría revelar información adicional (datos del sistema, información de depuración, etc.), que le ayudaría a conocer el sistema y a planificar nuevos ataques. Se ha reservado el identificador CVE-2019-0285 para esta vulnerabilidad.
- AP NetWeaver Java Application Server tiene una vulnerabilidad de suplantación, un atacante podría mostrar al usuario datos ilegibles, cambiar la dirección del remitente, los datos mostrados en una página y otra información importante. Se ha reservado el identificador CVE-2019-0283 para esta vulnerabilidad.

Los identificadores del resto de vulnerabilidades son: CVE-2019-0265, CVE-2019-0279, CVE-2019-0282, CVE-2019-0284, CVE-2019-0278 y CVE-2018-2484.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en BigFix Platform de IBM

Fecha de publicación: 10/04/2019

Importancia: Crítica

Recursos afectados:

- IBM BigFix Platform, desde la versión 9.5 hasta la 9.5.11

Descripción:

IBM ha publicado un boletín de seguridad que incluye múltiples vulnerabilidades en librerías OpenSSL, Query y YUI utilizadas por BigFix, y una vulnerabilidad crítica específica que podría permitir cargas no autorizadas en el sistema.

Solución:

- Aplicar el parche de actualización 9.5.12.
- Ejecutar el *Fixlet* de actualización asociado en la consola.

Detalle:

- IBM BigFix Platform podría permitir a un usuario autenticado subir un archivo al servidor con privilegios elevados, esto podría resultar en una ejecución no autorizada en el sistema subyacente. Se ha reservado el identificador CVE-2019-4013 para esta vulnerabilidad.
- El resto de vulnerabilidades son del tipo Simultaneous Multi-Threading (*SMT*) y *cross-site scripting* (*XSS*). Se han asignado los identificadores CVE-2018-5407, CVE-2012-5883, CVE-2012-6708 y CVE-2015-9251 para estas vulnerabilidades.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en Apache Tomcat

Fecha de publicación: 11/04/2019

Importancia: Alta

Recursos afectados:

- Apache Tomcat en la plataforma Windows, versiones:
  - Desde 7.0.0 hasta 7.0.93
  - Desde 8.5.0 hasta 8.5.39
  - Desde 9.0.0.M1 hasta 9.0.17

Descripción:

Esta vulnerabilidad fue identificada por un investigador de seguridad externo. Posteriormente, el equipo de seguridad de Apache Tomcat fue informado a través del programa *bug bounty* patrocinado por el proyecto EU FOSSA-2 el 3 de marzo de 2019, y se publicó el 10 de abril de 2019.

Solución:

- Actualizar a la versión 7.0.94 o superior.
- Actualizar a la versión 8.5.40 o superior.
- Actualizar a la versión 9.0.18 o superior.

Detalle:

- Cuando se ejecuta en Windows con *enableCmdLineArguments* activado, el Servlet CGI es vulnerable a una ejecución remota de código (RCE) debido a un error en la forma en que el JRE pasa a Windows los argumentos de la línea de comandos. El Servlet CGI está deshabilitado por defecto. La opción de CGI *enableCmdLineArguments* está desactivada por defecto en Tomcat 9.0.x. Se ha asignado el identificador CVE-2019-0232 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Vulnerabilidad de inyección de comandos en Citrix

Fecha de publicación: 11/04/2019

Importancia: Crítica

Recursos afectados:

- NetScaler SD-WAN Center 9.x, todas las versiones
- NetScaler SD-WAN Center, todas las versiones 10.0.x anteriores a 10.0.7
- Citrix SD-WAN Center, 10.1.x todas las versiones
- Citrix SD-WAN Center, todas las versiones 10.2.x anteriores a 10.2.1

Descripción:

Citrix ha publicado una vulnerabilidad de inyección de comandos que afecta a dos de sus productos.

Solución:

- NetScaler SD-WAN Center, actualizar a la versión 10.0.7 o superior.
- Centro Citrix SD-WAN, actualizar a la versión 10.2.1 o superior.

Detalle:

- La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado con acceso a la consola de administración poner en peligro el *host*. Se ha reservado el identificador CVE-2019-10883 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en BIG-IP de F5

Fecha de publicación: 11/04/2019

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 - 14.1.0.1
  - 13.0.0 - 13.1.1.3
  - 12.10 - 12.1.4
  - 11.6.1 - 11.6.3
  - 11.5.1 - 11.5.8

Descripción:

F5 ha publicado múltiples vulnerabilidades del tipo XSS, denegación de servicio y almacenamiento inseguro de claves.

Solución:

- Actualizar a las siguientes versiones:
  - 14.1.0.2
  - 13.1.1.4
  - 12.1.4.1
  - 11.6.4
  - 11.5.9

Detalle:

- Los atributos *tooltip* y *popover data-template* en *Bootstrap* permiten ataques XSS. Se ha asignado el identificador CVE-2019-8331 para esta vulnerabilidad de severidad alta.
- El sistema BIG-IP es vulnerable a un ataque de denegación de servicio (DoS) cuando se realiza la clasificación de URL utilizando el módulo APM. Se ha reservado el identificador CVE-2019-6610 para esta vulnerabilidad de severidad alta.
- En las plataformas *iSeries*, el atributo *secureKeyCapable* no está establecido, lo que hace que la función *Secure Vault* no utilice la compatibilidad con el hardware F5 para almacenar la clave de la unidad. Como resultado, la clave de la unidad se almacena en texto plano. Se ha reservado el identificador CVE-2019-6609 para esta vulnerabilidad de severidad media.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Juniper

Fecha de publicación: 11/04/2019

Importancia: Crítica

Recursos afectados:

- Service Insight versiones desde 15.1R1 y previas a 18.1R1
- Versiones de Service Now versiones desde 15.1R1 y previas a 18.1R1
- Juniper Identity Management Service versiones previas a 1.1.4
- Junos OS:
  - 12.1X46 versiones anteriores e incluyendo 12.1X46-D25, previas a 12.1X46-D71, 12.1X46-D73, 12.1X46-D77 en la serie SRX
  - 12.1X46 versiones anteriores a 12.1X46-D82 en la serie SRX5000
  - 12.3 versiones anteriores a 12.3R12-S10
  - 12.3X48 versiones anteriores a 12.3X48-D50 y 12.3X48-D75 en la serie SRX
  - 12.3X48 versiones anteriores a 12.3X48-D80 en la serie SRX5000
  - 14.1X53 en la serie QFX5000, EX4300, EX4600
  - 14.1X53 versiones anteriores a 14.1X53-D130, 14.1X53-D49
  - 14.1X53 versiones anteriores a 14.1X53-D48 en la serie EX / QFX
  - 15.1 versiones anteriores a 15.1F6-S12, 15.1R7-S3 y 15.1R7-S4
  - 15.1 versiones anteriores a 15.1R4-S9, 15.1R7-S2
  - 15.1F6 versiones anteriores a 15.1F6-S11
  - 15.1X49 versiones anteriores a 15.1X49-D141, 15.1X49-D144, 15.1X49-D150 en la serie SRX
  - 15.1X49 versiones anteriores a 15.1X49-D160 en SRX340 / SRX345
  - 15.1X49 versiones anteriores a 15.1X49-D160 en la serie SRX5000
  - 15.1X49 versiones anteriores a 15.1X49-D160, 15.1X49-D161, 15.1X49-D170, 15.1X49-D171, 15.1X49-D180
  - 15.1X49 versiones anteriores a 15.1X49-D75 en la serie SRX.
  - 15.1X53 versiones anteriores a 15.1X53-D234 en las series QFX5200 / QFX5110
  - 15.1X53 versiones anteriores a 15.1X53-D235 en la serie QFX5000, EX4300, EX4600
  - 15.1X53 versiones anteriores a 15.1X53-D236, 15.1X53-D495, 15.1X53-D496, 15.1X53-D591, 15.1X53-D69, 15.1X53-D68
  - 15.1X53 versiones anteriores a 15.1X53-D471, 15.1X53-D490 en la serie NFX
  - 15.1X53 versiones anteriores a 15.1X53-D590 en las series EX2300 / EX3400
  - 15.1X53 versiones anteriores a 15.1X53-D68 en la serie QFX10K
  - 15.1X54 en la serie ACX
  - 16.1 versiones anteriores a 16.1R3-S10, 16.1R4-S12, 16.1R4-S11, 16.1R6-S5, 16.1R6-S6, 16.1R7-S4, 16.1R7-S3, 16.1R7, 16.1R7-S5, 16.1R7-S1
  - 16.1X65 versiones anteriores a 16.1X65-D49, 16.1X65-D48
  - 16.2 versiones anteriores a 16.2R2-S6, 16.2R2-S7, 16.2R2-S8, 16.2R2-S9, 16.2R3
  - 17.1 versiones anteriores a 17.1R2-S10, 17.1R2-S8, 17.1R2-S7, 17.1R3
  - 17.1 versiones anteriores a 17.1R3 en la serie QFX5000, EX4300, EX4600
  - 17.2 versiones anteriores a 17.2R1-S7, 17.2R1-S8, 17.2R3, 17.2R3-S1
  - 17.2 versiones anteriores a 17.2R3 en la serie QFX5000, EX4300, EX4600
  - 17.2X75 versiones anteriores a 17.2X75-D92, 17.2X75-D102, 17.2X75-D110
  - 17.3 en SRX340 / SRX345
  - 17.3 versiones anteriores a 17.3R2, 17.3R2-S2, 17.3R3
  - 17.3 versiones anteriores a 17.3R3-S2, 17.3R4 en la serie QFX5000, EX4300, EX4600
  - 17.3 versiones anteriores a 17.3R3-S3, 17.3R3-S4, 17.3R4

- 17.4 versiones anteriores a 17.4R1-S1, 17.4R2-S2, 17.4R2-S3, 17.4R2-S4, 17.4R1-S4, 17.4R1-S6, 17.4R1-S7, 17.4R2, 17.4R2-S3, 17.4R3
- 17.4 versiones anteriores a 17.4R2-S1, 17.4R3 en la serie QFX5000, EX4300, EX4600
- 17.4 versiones anteriores a 17.4R2-S3, 17.4R3 en SRX340 / SRX345
- 18.1 versiones anteriores a 18.1R2, 18.1R3-S1, 18.1R3-S2, 18.1R3-S3, 18.1R3-S4, 18.1R4
- 18.1 versiones anteriores a 18.1R3-S1 en SRX340 / SRX345
- 18.1 versiones anteriores a 18.1R3-S1, 18.1R4 en la serie QFX5000, EX4300, EX4600
- 18.2 versiones anteriores a 18.2R1-S5, 18.2R2-S1
- 18.2 versiones anteriores a 18.2R2 en la serie QFX5000, EX4300, EX4600
- 18.2 versiones anteriores a 18.2R2 en SRX340 / SRX345
- 18.2 versiones anteriores a 18.2R2, 18.2R2-S2, 18.2R2-S3, 18.2R3
- 18.2 versiones anteriores a 18.2R1-S2, 18.2R2 en la serie EX4300-MP
- 18.2X75 versiones anteriores a 18.2X75-D10, 18.2X75-D30, 18.2X75-D40
- 18.2X75 versiones anteriores a 18.2X75-D30 en la serie QFX5000, EX4300, EX4600
- 18.3 versiones anteriores a 18.3R1-S1, 18.3R1-S3, 18.3R1-S2, 18.3R1-S3, 18.3R2
- 18.3 versiones anteriores a 18.3R1-S2, 18.3R2 en SRX340 / SRX345
- 18.3 versiones anteriores a 18.3R2 en la serie QFX5000, EX4300, EX4600
- 18.4 versiones anteriores a 18.4R1-S1, 18.4R1-S2, 18.4R2
- Todas las versiones anteriores e inclusive 12.3

Descripción:

Juniper ha publicado 17 avisos de seguridad que contienen 17 vulnerabilidades, 1 de severidad crítica, 9 de criticidad alta y el resto medias o bajas.

Solución:

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

Detalle:

- La vulnerabilidad de severidad crítica afecta a Junos Networks Junos OS en la serie QFX5000, EX4300, EX4600. Una determinada secuencia de paquetes BGP o IPv6 BFD válidos puede desencadenar un desbordamiento de búfer basado en pila en Junos OS Forwarding Engine Manager (FXPC), en los dispositivos de la serie QFX5000, EX4300, EX4600. Este problema puede ocasionar un cierre inesperado del daemon fxpc o la ejecución remota de código. Se ha asignado el identificador CVE-2019-0008 a esta vulnerabilidad.

El resto de vulnerabilidades podrian originar:

- Omisión en el firewall, se les han asignado los identificadores CVE-2019-0036 y CVE-2019-0042
- Denegación de servicio (DoS), se les han asignado los identificadores CVE-2019-0044, CVE-2019-0031, CVE-2019-0033, CVE-2019-0037, CVE-2019-0019, CVE-2019-0028, CVE-2019-0043, CVE-2019-0038, CVE-2019-0040 y CVE-2019-0042
- Credenciales almacenadas en texto plano, se les han asignado los identificadores CVE-2019-0032
- Acceso a información privilegiada, se le ha asignado el identificador CVE-2019-0034
- Omisión de autenticación, se le ha asignado el identificador CVE-2019-0035
- Obtención de credenciales por fuerza bruta, se les han asignado los identificadores CVE-2019-0039
- Acceso al plano de control a través de la interfaz *loopback*, se le ha asignado el identificador CVE-2019-0041

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en API Connect de IBM

Fecha de publicación: 12/04/2019

Importancia: Crítica

Recursos afectados:

- IBM API Connect, versiones desde 5.0.0.0 hasta 5.0.8.6

Descripción:

Se han publicado dos vulnerabilidades de tipo inyección de comandos e inclusión de archivos locales (LFI, *Local File Inclusion*) en API Connect.

Solución:

- IBM ha solucionado ambas vulnerabilidades en la versión 5.0.8.6 *iFix*.

Detalle:

- IBM API Connect Developer Portal es vulnerable a la inyección de comandos. Un atacante que realice una petición especialmente diseñada puede ejecutar código arbitrario en el servidor y obtener acceso completo al sistema. Se ha reservado el identificador CVE-2019-4202 para esta vulnerabilidad.
- IBM API Connect Developer Portal puede ser aprovechado por los desarrolladores de aplicaciones para descargar archivos arbitrarios del sistema operativo del *host* y llevar a cabo ataques SSRF (*Server Side Request Forgery*). Se ha reservado el identificador CVE-2019-4203 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades de lectura fuera de límites en productos VMware

Fecha de publicación: 12/04/2019

Importancia: Alta

Recursos afectados:

- VMware vSphere ESXi (ESXi) versiones:
  - 6.5
  - 6.7
- VMware Workstation Pro / Player (Workstation) versiones:
  - 15.X
  - 14.X
- VMware Fusion Pro / Fusion (Fusion) versiones:
  - 11.x
  - 10.x

Descripción:

VMware ha detectado 3 vulnerabilidades de criticidad alta del tipo lectura fuera de límites que afectan a varios de sus productos.

Solución:

VMware ha publicado diversas actualizaciones, en función del producto y versión afectada, que mitigan las vulnerabilidades.

- ESXi versiones:
  - 6.7 aplicar el parche ESXi670-201904101-SG
  - 6.5 aplicar el parche ESXi650-201903001
- Workstation Pro actualizar a las versiones 14.1.6 o 15.0.3
- Workstation Player actualizar a las versiones 14.1.6 o 15.0.3
- Fusion Pro / Fusion actualizar a las versiones 10.1.6 o 11.0.3

Detalle:

- Una vulnerabilidad de lectura fuera de límites en la funcionalidad *vertex shader* podría permitir a un atacante, que accediese a una máquina virtual con los gráficos 3D habilitados, revelar información o generar una condición de denegación de servicio en la máquina virtual. Se ha reservado el identificador CVE-2019-5516 para esta vulnerabilidad.
- Múltiples vulnerabilidades del tipo lectura fuera de límites en *shader translator* podrían permitir a un atacante, que accediese a una máquina virtual con los gráficos 3D habilitados, revelar información o generar una condición de denegación de servicio en la máquina virtual. Se ha reservado el identificador CVE-2019-5517 para esta vulnerabilidad.
- Una vulnerabilidad de lectura fuera de límites podría permitir a un atacante, que accediese a una máquina virtual con los gráficos 3D habilitados, revelar información o generar una condición de denegación de servicio en la máquina virtual. Se ha reservado el identificador CVE-2019-5520 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Actualizaciones críticas en Oracle (abril 2019)

Fecha de publicación: 17/04/2019

Importancia: Crítica

Recursos afectados:

- Agile Recipe Management for Pharmaceuticals, versiones 9.3.3 y 9.3.4
- Enterprise Manager Base Platform, versiones 12.1.0.5.0, 13.2.0.0.0 y 13.3.0.0.0
- Enterprise Manager Ops Center, versión 12.3.3
- FMW Platform, versión 12.2.1.3.0
- Instantis EnterpriseTrack, versiones 17.1, 17.2 y 17.3
- JD Edwards EnterpriseOne Tools, versión 9.2
- JD Edwards World Technical Foundation, versiones A9.2, A9.3.1 y A9.4
- MICROS Lucas, versiones 2.9.5.6 y 2.9.5.7
- MICROS Relate CRM Software, versión 11.4
- MICROS Retail-J, versión 12.1.2
- MySQL Connectors, versiones 5.3.12 y anteriores, y 8.0.15 y anteriores
- MySQL Enterprise Backup, versiones 3.12.3 y anteriores, y 4.1.2 y anteriores
- MySQL Enterprise Monitor, versiones 4.0.8 y anteriores, 8.0.14 y anteriores
- MySQL Server, versiones 5.6.43 y anteriores, 5.7.25 y anteriores, 8.0.15 y anteriores
- Oracle Agile PLM, versiones 9.3.3, 9.3.4 y 9.3.5
- Oracle API Gateway, versión 11.1.2.4.0
- Oracle Application Testing Suite, versión 13.3.0.1
- Oracle AutoVue 3D Professional Advanced, versiones 21.0.0 y 21.0.1
- Oracle Banking Platform, versiones 2.4.0, 2.4.1, 2.5.0 y 2.6.0
- Oracle Berkeley DB, versiones anteriores a 6.138 y versiones anteriores a 18.1.32
- Oracle BI Publisher, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0
- Oracle Business Process Management Suite, versiones 11.1.1.9.0, 12.1.3.0.0 y 12.2.1.3.0
- Oracle Business Transaction Management, versión 12.1.0
- Oracle Commerce Merchandising, versión 11.2.0.3
- Oracle Commerce Platform, versiones 11.2.0.3 y 11.3.1
- Oracle Communications Application Session Controller, versiones 3.7.1 y 3.8.0
- Oracle Communications EAGLE Application Processor, versiones 16.1.0 y 16.2.0
- Oracle Communications EAGLE LNP Application Processor, versiones 10.0, 10.1 y 10.2
- Oracle Communications Instant Messaging Server, versión 10.0.1
- Oracle Communications Interactive Session Recorder, versiones 6.0, 6.1 y 6.2
- Oracle Communications LSMS, versiones 13.1, 13.2 y 13.3
- Oracle Communications Messaging Server, versiones 8.0 y 8.1
- Oracle Communications Operations Monitor, versiones 3.4 y 4.0
- Oracle Communications Policy Management, versiones 12.1, 12.2, 12.3 y 12.4
- Oracle Communications Pricing Design Center, versiones 11.1 y 12.0
- Oracle Communications Service Broker, versión 6.0
- Oracle Communications Service Broker Engineered System Edition, versión 6.0
- Oracle Communications Session Border Controller, versiones 8.0.0, 8.1.0 y 8.2.0
- Oracle Communications Unified Inventory Management, versiones 7.3.2, 7.3.4, 7.3.5 y 7.4.0
- Oracle Configuration Manager, versión 12.1.0
- Oracle Configurator, versiones 12.1 y 12.2

- Oracle Data Integrator, versiones 11.1.1.9.0 y 12.2.1.3.0
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c y 19c
- Oracle E-Business Suite, versiones 0.9.8, 1.0.0, 1.0.1, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 y 12.2.8
- Oracle Endeca Information Discovery Integrator, versión 3.2.0
- Oracle Enterprise Communications Broker, versiones 3.0.0 y 3.1.0
- Oracle Enterprise Operations Monitor, versiones 3.4 y 4.0
- Oracle Enterprise Session Border Controller, versiones 8.0.0, 8.1.0 y 8.2.0
- Oracle Financial Services Analytical Applications Infrastructure, versiones 7.3.3 - 7.3.5 y 8.0.0 - 8.0.7
- Oracle Financial Services Asset Liability Management, versiones 8.0.4 - 8.0.7
- Oracle Financial Services Data Integration Hub, versiones 8.0.5 - 8.0.7
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.4 - 8.0.7
- Oracle Financial Services Hedge Management y IFRS Valuations, versiones 8.0.4 - 8.0.7
- Oracle Financial Services Liquidity Risk Management, versiones 8.0.2 - 8.0.6
- Oracle Financial Services Loan Loss Forecasting y Provisioning, versiones 8.0.2 - 8.0.7
- Oracle Financial Services Market Risk Measurement y Management, versiones 8.0.5, 8.0.6
- Oracle Financial Services Profitability Management, versiones 8.0.4 - 8.0.6
- Oracle Financial Services Reconciliation Framework, versiones 8.0.5, 8.0.6
- Oracle FLEXCUBE Private Banking, versiones 2.0.0.0, 2.2.0.1, 12.0.1.0, 12.0.3.0 y 12.1.0.0
- Oracle Fusion Middleware MapViewer, versión 12.2.1.3.0
- Oracle Health Sciences Data Management Workbench, versión 2.4.8
- Oracle Healthcare Master Person Index, versiones 3.0 y 4.0
- Oracle Hospitality Cruise Dining Room Management, versión 8.0.80
- Oracle Hospitality Cruise Fleet Management, versión 9.0.11
- Oracle Hospitality Guest Access, versiones 4.2.0 y 4.2.1
- Oracle Hospitality Reporting y Analytics, versión 9.1.0
- Oracle HTTP Server, versión 12.2.1.3.0
- Oracle Identity Analytics, versión 11.1.1.5.8
- Oracle Java SE, versiones 7u211, 8u202, 11.0.2 y 12
- Oracle Java SE Embedded, versión 8u201
- Oracle JDeveloper, versiones 11.1.1.9.0, 12.1.3.0.0 y 12.2.1.3.0
- Oracle Knowledge, versiones 8.5.1.0 - 8.5.1.7, 8.6.0 y 8.6.1
- Oracle Managed File Transfer, versiones 12.1.3.0.0 y 12.2.1.3.0
- Oracle Outside In Technology, versiones 8.5.3 y 8.5.4
- Oracle Real-Time Scheduler, versión 2.3.0
- Oracle Retail Allocation, versión 15.0.2
- Oracle Retail Convenience Store Back Office, versión 3.6
- Oracle Retail Customer Engagement, versiones 16.0 y 17.0
- Oracle Retail Customer Management y Segmentation Foundation, versiones 16.0, 17.0 y 18.0
- Oracle Retail Invoice Matching, versiones 12.0, 13.0, 13.1, 13.2, 14.0, 14.1 y 15.0
- Oracle Retail Merchandising System, versiones 15.0 y 16.0
- Oracle Retail Order Broker, versiones 5.1, 5.2, 15.0 y 16.0
- Oracle Retail Point-of-Service, versiones 13.4, 14.0 y 14.1
- Oracle Retail Workforce Management Software, versión 1.60.9.0.0
- Oracle Retail Xstore Point of Service, versiones 7.0 y 7.1
- Oracle Secure Global Desktop, versión 5.4
- Oracle Service Bus, versiones 11.1.1.9.0, 12.1.3.0.0 y 12.2.1.3.0
- Oracle SOA Suite, versiones 11.1.1.9.0, 12.1.3.0.0 y 12.2.1.3.0
- Oracle Solaris, versiones 10 y 11
- Oracle Traffic Director, versión 11.1.1.9.0
- Oracle Transportation Management, versiones 6.3.7, 6.4.2 y 6.4.3
- Oracle Tuxedo, versión 12.1.1.0.0
- Oracle Utilities Framework, versiones 2.2.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.2.0, 4.3.0.3.0, 4.3.0.4.0, 4.3.0.5.0, 4.3.0.6.0 y 4.4.0.0.0
- Oracle Utilities Mobile Workforce Management, versión 2.3.0
- Oracle Utilities Network Management System, versión 1.12.0.3
- Oracle VM VirtualBox, versiones anteriores a 5.2.28 y anteriores a 6.0.6
- Oracle WebCenter Portal, versión 12.2.1.3.0
- Oracle WebCenter Sites, versión 12.2.1.3.0
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0 y 12.2.1.3.0
- OSS Support Tools, versión 19.1
- PeopleSoft Enterprise ELM, versión 9.2
- PeopleSoft Enterprise ELM Enterprise Learning Management, versión 9.2
- PeopleSoft Enterprise HCM Talent Acquisition Manager, versión 9.2
- PeopleSoft Enterprise HRMS, versión 9.2
- PeopleSoft Enterprise PeopleTools, versiones 8.55, 8.56 y 8.57
- PeopleSoft Enterprise PT PeopleTools, versiones 8.55, 8.56 y 8.57
- Primavera P6 Enterprise Project Portfolio Management, versiones 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12 y 18.8
- Primavera Unifier, versiones 16.1, 16.2, 17.7 - 17.12 y 18.8
- Siebel Applications, versión 19.3

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 297 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, Virtualización, Vulnerabilidad

---

Múltiples vulnerabilidades en BIND

Fecha de publicación: 25/04/2019

Importancia: Alta

Recursos afectados:

- BIND, versiones desde la 9.9.0 hasta la 9.10.8-P1, desde la 9.11.0 hasta la 9.11.6, desde la 9.12.0 hasta la 9.12.4 y 9.14.0.
- BIND 9 Supported Preview Edition, versiones desde la 9.9.3-S1 hasta la 9.11.5-S3, y 9.11.5-S5. Las versiones desde la 9.13.0 hasta la 9.13.7 de la rama de desarrollo 9.13 también se ven afectadas. Las versiones anteriores a BIND 9.9.0 no han sido evaluadas por la vulnerabilidad CVE-2018-5743.
- BIND Supported Preview Edition, versiones desde la 9.10.5-S1 hasta la 9.11.5-S5.

Descripción:

Se han publicado múltiples vulnerabilidades en BIND que afectan a varios de sus productos, 1 de severidad alta y 2 de severidad media.

Solución:

En función de la versión afectada actualizar a la versión que corresponda.

- BIND 9.11.5-S6
- BIND 9.11.6-S1
- BIND 9.11.6-P1
- BIND 9.12.4-P1
- BIND 9.14.1

Detalle:

- Por diseño, BIND limita el número de clientes TCP que se pueden conectar de forma simultánea, este parámetro es ajustable, pero si no se ajusta tiene un valor conservador. Un error en el código podría permitir a un atacante aumentar el número de conexiones TCP simultáneas más allá del límite, originando un agotamiento del conjunto de descriptores de archivos disponibles para las conexiones de red. Se ha reservado el identificador CVE-2018-5743 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los identificadores CVE-2019-6467 y CVE-2019-6468.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de TIBCO

Fecha de publicación: 25/04/2019

Importancia: Crítica

Recursos afectados:

- TIBCO ActiveMatrix BPM, versiones 4.2.0 y anteriores.
- TIBCO ActiveMatrix BPM Distribution para TIBCO Silver Fabric, versiones 4.2.0 y anteriores.
- TIBCO ActiveMatrix Policy Director, versiones 1.1.0 y anteriores.
- TIBCO ActiveMatrix Service Bus, versiones 3.3.0 y anteriores.
- TIBCO ActiveMatrix Service Grid, versiones 3.3.1 y anteriores.
- TIBCO ActiveMatrix Service Grid Distribution para TIBCO Silver Fabric, versiones 3.3.0 y anteriores.
- TIBCO Silver Fabric Enabler para ActiveMatrix BPM, versiones 1.4.1 y anteriores.
- TIBCO Silver Fabric Enabler para ActiveMatrix Service Grid, versiones 1.3.1 y anteriores.
- Componentes de interfaz web del administrador, servidor de administración, servidor web administrativo, área de trabajo del cliente, espacio abierto del cliente, cliente de desarrollo de aplicaciones y REST API.

Descripción:

TIBCO ha publicado 6 vulnerabilidades que afectan a varios de sus productos, en las que un atacante podría realizar ataques XSS, CSRF, ejecución remota de código, descarga de información confidencial sin autenticación, escalada de privilegios o redirección abierta.

Solución:

- TIBCO ActiveMatrix BPM, actualizar a la versión 4.3.0 o superior.
- TIBCO ActiveMatrix BPM Distribution para TIBCO Silver Fabric, actualizar a la versión 4.3.0 o superior.
- TIBCO ActiveMatrix Policy Director, actualizar a la versión 2.0.0 o superior. Debido a la retirada programada de este producto a principios de 2021, se recomienda encarecidamente a los clientes que se pongan en contacto con el servicio de asistencia técnica de TIBCO para explorar vías alternativas de reparación.
- TIBCO ActiveMatrix Service Bus, actualizar a la versión 3.4.0 o superior.
- TIBCO ActiveMatrix Service Grid, actualizar a la versión 3.4.0 o superior.
- TIBCO ActiveMatrix Service Grid Distribution para TIBCO Silver Fabric, actualizar a la versión 3.4.0 o superior.
- TIBCO Silver Fabric Enabler para ActiveMatrix BPM, actualizar a la versión 1.4.2 o superior.
- TIBCO Silver Fabric Enabler para ActiveMatrix Service Grid, actualizar a la versión 1.3.2 o superior.

Detalle:

- Un atacante remoto sin privilegios podría obtener acceso completo a todas las capacidades de la interfaz web de TIBCO ActiveMatrix Administrator a través de XSS o CSRF. Se ha asignado el identificador CVE-2019-8991 para esta vulnerabilidad.
- Un usuario sin privilegios puede cargar código, lo que le permitiría ejecutar código arbitrario en los nodos de ActiveMatrix Service Grid. Se ha asignado el identificador CVE-2019-8992 para esta vulnerabilidad.
- Un usuario no autenticado podría descargar un archivo con información de credenciales. Se ha asignado el identificador CVE-2019-8993 para esta vulnerabilidad.
- Un usuario autenticado podría engañar a otros usuarios del sistema para que visiten sitios web maliciosos. Se ha asignado el identificador CVE-2019-8994 para esta vulnerabilidad.
- Un atacante podría utilizar una URL maliciosa para engañar a un usuario y que visite un sitio web específico. Se ha asignado el identificador CVE-2019-8995 para esta vulnerabilidad.
- Un atacante remoto sin privilegios podría obtener acceso completo a las API expuestas por los componentes de ActiveMatrix BPM afectados. Se ha asignado el identificador CVE-2019-11203 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de inyección de cabeceras de host en IBM StoredIQ

Fecha de publicación: 29/04/2019

Importancia: Alta

Recursos afectados:

- IBM StoredIQ, versiones desde 7.6.0.0 hasta 7.6.0.18

Descripción:

IBM StoredIQ se ve afectado por una posible inyección de cabeceras de *host* en StoredIQ Dataserver.

Solución:

- No es necesario realizar ninguna corrección, pero la configuración debe actualizarse tal y como se describe en la sección *Workarounds and Mitigations* del aviso de IBM referenciado.

Detalle:

- IBM StoredIQ 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, el atacante remoto podría explotar esta vulnerabilidad falsificando la URL mostrada y redirigiendo al usuario a un sitio web malicioso aparentemente confiable. Esto podría permitir al atacante obtener información sensible o realizar nuevos ataques contra la víctima. Se ha reservado el identificador CVE-2019-4166 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en Oracle WebLogic Server

Fecha de publicación: 29/04/2019

Importancia: Crítica

Recursos afectados:

- Oracle WebLogic Server, versiones 10.3.6.0.0 y 12.1.3.0.0

Descripción:

Oracle ha publicado una vulnerabilidad de severidad crítica que permite la ejecución remota de código en su producto Oracle WebLogic Server y para la cual ya hay una prueba de concepto de su explotación.

Solución:

- Oracle ha puesto a disposición de los usuarios un enlace para acceder a la documentación que contiene información sobre la disponibilidad de parches e instrucciones de instalación.
- Como medida de mitigación, se recomienda desactivar los módulos vulnerables «wls9_async_response.war» y «wls-wsat.war», o inhibir el acceso a las URL «/ _async / *» y «/ wls-wsat / *» dentro de las instalaciones de Oracle WebLogic.

Detalle:

- Una vulnerabilidad de tipo deserialización en Oracle WebLogic Server, podría permitir a un atacante de forma remota y sin autenticación la ejecución de código. Se ha asignado el identificador CVE-2019-2725 para esta vulnerabilidad.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Salto de autenticación en XenMobile Server de Citrix

Fecha de publicación: 29/04/2019

Importancia: Crítica

Recursos afectados:

- Citrix XenMobile Server versiones:
  - 10.9.0 anteriores al *Rolling Patch* 3.
  - 10.8.0 anteriores al *Rolling Patch* 6.

Descripción:

Se ha identificado una vulnerabilidad de severidad crítica en Citrix XenMobile Server del tipo salto de autenticación.

Solución:

- Citrix ha publicado actualizaciones para sus usuarios registrados que mitigan la vulnerabilidad:
  - Citrix XenMobile Server 10.9.0 *Rolling Patch 3*
  - Citrix XenMobile Server 10.8.0 *Rolling Patch 6*

Detalle:

- La vulnerabilidad podría permitir a un atacante realizar un salto de autenticación en Citrix XenMobile Server y tomar acciones en cualquier dispositivo registrado en el *Mobile Device Management* (MDM). Se ha reservado identificador CVE-2018-18571 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad DoS en Liferay

Fecha de publicación: 29/04/2019

Importancia: Alta

Recursos afectados:

- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6
- liferay-faces-bridge-impl-3.1.5-ga6
- liferay-faces-bridge-impl-3.0.5-ga6
- liferay-faces-bridge-impl-3.0.5-legacy-ga6
- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6
- liferay-faces-bridge-impl-3.1.5-ga6
- liferay-faces-bridge-impl-3.0.5-ga6
- liferay-faces-bridge-impl-3.0.5-legacy-ga6
- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6

Compatibles con algunas de estas versiones:

- Liferay Portal 5.2
- Liferay Portal 6.0
- Liferay Portal 6.1
- Liferay Portal 6.2
- Liferay Portal 7.0
- Liferay Portal 7.1
- Pluto Portal 2.0

Para más detalles, consulte las referencias.

Descripción:

Múltiples vulnerabilidades en Liferay Portal CE pueden provocar la denegación del servicio a través de la carga de archivos grandes.

Solución:

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

Detalle:

- Cuando se utiliza en conjunto con Liferay Faces Bridge, la validación de carga de archivos puede omitirse, lo que permite cargar archivos muy grandes que se pueden utilizar en un ataque de denegación de servicio (DoS). Los archivos que se omiten durante la validación son:
  - PrimeFaces 6.2 p:fileUpload.
  - RichFaces rich:fileUpload.
  - com.liferay.faces.bridge.uploadedFileMaxSize on IceFaces ace:fileEntry.
  - com.liferay.faces.util.uploadedFileMaxSize con alloy:inputFile en Portlets.
  - IceFaces 1.8 ice:inputFile.

Etiquetas: Vulnerabilidad