Boletín de octubre de 2019

Avisos Técnicos

Múltiples vulnerabilidades en productos de HPE

Fecha de publicación: 01/10/2019

Importancia: Crítica

Recursos afectados:

- HPE UIoT, versión 1.2.4.2;
- Simplivity OmniCube, versiones desde 3.0.7 hasta 3.7.9;
- SimpliVity 380, versiones desde 3.0.7 hasta 3.7.9;
- SimpliVity 2600;
- SimpliVity OmniStack para Dell, Lenovo y Cisco.

Descripción:

El equipo de respuesta de seguridad de HPE ha descubierto múltiples vulnerabilidades en varios productos del fabricante.

Solución:

- Para UIoT, versión 1.2.4.2 y anteriores, actualizar a 1.2.4.2 RP3 HF1;
- Para Simplivity, actualizar OmniStack a la versión 3.7.10.

Detalle:

- HPE UIoT contiene una vulnerabilidad que podría permitir a un atacante remoto acceso no autorizado o revelar información confidencial del usuario. Se ha reservado el identificador CVE-2019-11995 para esta vulnerabilidad.
- Una vulnerabilidad detectada en múltiples versiones de SimpliVity permitiría a un atacante, tanto de manera local como remota, realizar modificaciones o eliminaciones de archivos arbitrarios en los nodos con privilegios de *root*, a través de llamadas a APIs obsoletas. Se ha reservado el identificador CVE-2019-11993 para esta vulnerabilidad.

Etiquetas: Actualización, HP, IoT, Vulnerabilidad

Múltiples vulnerabilidades en Security Directory Server de IBM

Fecha de publicación: 02/10/2019

Importancia: Alta

Recursos afectados:

Security Directory Server, versión 6.4.0.

Descripción:

El equipo *X-Force Ethical Hacking* de IBM ha descubierto cinco vulnerabilidades, tres con criticidades altas y dos con criticidades medias. Un atacante remoto podría revelar información sensible, modificar archivos, robo de credenciales u obtener información del sistema.

Solución:

Actualizar a la versión 6.4.0.19-ISS-ISDS-IF0019.

Detalle:

Las vulnerabilidades con criticidades altas:

- Un uso inadecuado de los ajustes de cierre de cuenta podría permitir a un atacante remoto obtener información de la cuenta de usuario mediante ataques de fuerza bruta. Se ha reservado el identificador CVE-2019-4520 para esta vulnerabilidad.
- Un ataque de redireccionamiento abierto podría permitir a un atacante remoto realizar un *phishing* y persuadir a la víctima para obtener información sensible. Se ha reservado el identificador CVE-2019-4538 para esta vulnerabilidad.
- Al procesar archivos XML, es posible no neutralizar correctamente ciertos elementos. Un atacante podría realizar modificaciones en la sintaxis, contenido o comandos en los XML antes de ser procesados por el sistema final. Se ha reservado el identificador CVE-2019-4539 para esta vulnerabilidad.

Para las vulnerabilidades con criticidades medias, se han reservado los identificadores CVE-2019-4542 y CVE-2019-4549.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de Palo Alto Networks

Fecha de publicación: 02/10/2019

Importancia: Alta

Recursos afectados:

Zingbox Inspector, versiones 1.280, 1.286, 1.288, 1.294 y anteriores.

Descripción:

Se han publicado varias vulnerabilidades de severidad alta que podrían permitir a un atacante la ejecución arbitraria de código, el uso de credenciales embebidas, la inserción de información en la base de datos o la evasión de autenticación.

Solución:

Actualizar a la versión 1.295 o posterior.

Detalle:

- La vulnerabilidad de inyección de comandos en el Zingbox Inspector CLI, podría permitir a un usuario autenticado ejecutar comandos arbitrarios del sistema. Se ha reservado el identificador CVE-2019-15014 para esta vulnerabilidad.
- Los usuarios podrían autenticarse en el software utilizando credenciales con código embebido si el acceso a SSH en el Zingbox Inspector no está restringido con medidas adicionales. Se han reservado los identificadores CVE-2019-15015 y CVE-2019-15017 para estas vulnerabilidades.
- Los usuarios autenticados podrían insertar comandos no saneados a la base de datos de Zingbox Inspector backend, lo que puede causar problemas u otros daños a la base de datos o al sistema. Se ha reservado el identificador CVE-2019-15016 para esta vulnerabilidad.
- Zingbox Inspector no requiere autenticación cuando se vincula la instancia del Inspector a un cliente diferente. Se ha reservado el identificador CVE-2019-15018 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Asignación incorrecta de permisos en múltiples productos de Dell EMC

Fecha de publicación: 04/10/2019

Importancia: Alta

Recursos afectados:

- Dell EMC Avamar Server, versiones 7.4.1, 7.5.0, 7.5.1, 18.2 y 19.1;
- Dell EMC Integrated Data Protection Appliance (IDPA), versiones 2.0, 2.1, 2.2, 2.3 y 2.4.

Descripción:

Múltiples productos de Dell EMC contienen una vulnerabilidad, clasificada con severidad alta, de asignación incorrecta de permisos para recursos críticos.

Solución:

Dell recomienda aplicar distintos *hotfix*, según la versión de los productos afectados:

- Dell EMC Avamar Server:
  - 7.4.1;
  - 7.5.0;
  - 7.5.1;
  - 18.2;
  - 19.1.
- Dell EMC Integrated Data Protection Appliance (IDPA):
  - 2.0;
  - 2.1;
  - 2.2;
  - 2.3;
  - 2.4.

Detalle:

La vulnerabilidad se debe a una asignación incorrecta de permisos para recursos críticos. Un atacante remoto, autenticado, podría modificar o revelar información confidencial de las copias de seguridad del sistema afectado. Se ha reservado el identificador CVE-2019-

3765 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

API vulnerable a una escalada de privilegios en Sterling Connect:Direct para UNIX de IBM

Fecha de publicación: 07/10/2019

Importancia: Alta

Recursos afectados:

- IBM Sterling Connect:Direct para Unix versiones:
  - 6.0.0,
  - 4.3.0,
  - 4.2.0.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta. Un atacante remoto, autenticado, podría obtener acceso no autorizado al sistema.

Solución:

IBM ha publicado actualizaciones de seguridad que solucionan la vulnerabilidad en función de la versión afectada.

- Actualizar a la versión:
  - 6.0.0,
  - 4.3.0,
  - 4.2.0.

Para versiones anteriores a la 4.2.0, IBM recomienda actualizar a una versión que contenga la solución.

Detalle:

La vulnerabilidad se encuentra cuando un usuario autorizado, con privilegios limitados para Connect:Direct, substituya la implementación *getuid()* por una maliciosa a través de la API C/C para UNIX. Un atacante remoto, autenticado, podría obtener acceso no autorizado servidor. Se ha reservado el identificador CVE-2019-4529 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Actualización de seguridad de SAP de octubre de 2019

Fecha de publicación: 09/10/2019

Importancia: Crítica

Recursos afectados:

- SAP NetWeaver Process Integration:
  - AS2 Adapter, versiones 1.0 y 2.0;
  - B2B Toolkit, versiones 1.0 y 2.0.
- SAP Landscape Management enterprise edition, versión 3.0;
- SAP IQ, versión 16.1;
- SAP SQL Anywhere, versión 17.0;
- SAP Dynamic Tiering, versiones 1.0 y 2.0;
- SAP Customer Relationship Management (Email Management):
  - S4CRM, versiones 100 y 200;
  - BBPCRM, versiones 700, 701, 702, 712, 713 y 714.
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), versiones 420 y 430;
- SAP Financial Consolidation, versiones 10.0 y 10.1;
- SAP Kernel (RFC):
  - KRNL32NUC, KRNL32UC y KRNL64NUC, versiones 7.21, 7.21EXT, 7.22 y 7.22EXT;
  - KRNL64UC, versiones 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49 y 7.73;
  - KERNEL, versiones 7.21, 7.49, 7.53, 7.73 y 7.76.

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 7 notas de seguridad y 1 actualización, siendo 2 de ellas de severidad crítica, 1 alta, y 5 medias.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de *Cross-Site Scripting* (XSS);
- 1 vulnerabilidad de denegación de servicio;
- 1 vulnerabilidad de divulgación de información;

- 1 vulnerabilidad de falta de comprobación de autorización;
- 1 vulnerabilidad de falta de autenticación;
- 1 vulnerabilidad de otro tipo.

Las notas de seguridad calificadas como críticas y alta se refieren a:

- La configuración del adaptador AS2 permite dos proveedores de seguridad diferentes. Dependiendo del proveedor seleccionado, existe una vulnerabilidad de falta de autenticación que puede conducir al robo o manipulación de datos confidenciales, así como al acceso a funcionalidades administrativas y otras funciones privilegiadas. Se ha asignado el identificador CVE-2019-0379 para esta vulnerabilidad.
- SAP Landscape Management Enterprise permite la definición de operaciones personalizadas, cada una de ellas asignadas a un proveedor específico. También se pueden añadir más parámetros personalizados a dicho proveedor. Este producto es vulnerable a una divulgación de información si estos parámetros personalizados cumplen unas condiciones específicas. Se ha asignado el identificador CVE-2019-0380 para esta vulnerabilidad.
- Existe una vulnerabilidad en el algoritmo de búsqueda de archivos que afecta a distintos productos. El algoritmo busca en demasiados directorios, incluso si están fuera del ámbito de aplicación. La explotación de esta vulnerabilidad permitiría a un atacante leer, sobrescribir, eliminar y exponer archivos arbitrarios del sistema. También puede llevar al secuestro de DLL, así como a la elevación de privilegios. Se ha asignado el identificador CVE-2019-0381 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2019-0368, CVE-2019-0374, CVE-2019-0375, CVE-2019-0376, CVE-2019-0377, CVE-2019-0378, CVE-2019-0370, CVE-2019-0369, CVE-2019-0365 y CVE-2019-0367.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad de inyección de parámetros en Spectrum Scale de IBM

Fecha de publicación: 09/10/2019

Importancia: Alta

Recursos afectados:

- IBM Spectrum Scale:
  - Desde la versión 5.0.0.0 hasta la versión 5.0.3.2.
  - Desde la versión 4.2.0.0 hasta la versión 4.2.3.17.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta en uno de sus productos. Un atacante podría obtener privilegios de *root* en el sistema.

Solución:

- Para los productos con versiones desde la 5.0.0.0 hasta la 5.0.3.2, actualizar la versión 5.0.3.3.
- Para los productos con versiones desde la 4.2.0.0 hasta la 4.2.3.17, actualizar la versión 4.2.3.18.

Detalle:

La vulnerabilidad se debe a la inyección de parámetros en archivos *setuid*. Un atacante podría obtener privilegios de *root* en el sistema. Se ha reservado el identificador CVE-2019-4558 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de octubre de 2019

Fecha de publicación: 09/10/2019

Importancia: Crítica

Recursos afectados:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge (EdgeHTML-based),
- ChakraCore,
- Microsoft Office, Microsoft Office Services y Web Apps,
- SQL Server Management Studio,
- Open Source Software,
- Microsoft Dynamics 365,
- Windows Update Assistant.

Descripción:

La publicación mensual de actualizaciones de seguridad de Microsoft consta de 59 vulnerabilidades, 10 clasificadas como críticas y 49 como importantes, siendo el resto de severidad media o baja.

Solución:

Instalar la actualización correspondiente. En la página de información de instalación de las actualizaciones de seguridad, se informa de los distintos métodos de actualización.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- denegación de servicio,
- escalada de privilegios,
- divulgación de información,
- ejecución remota de código,
- omisión de la característica de seguridad,
- suplantación,
- falsificación.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Ejecución remota de código en Dameware Mini Remote Control de SolarWinds

Fecha de publicación: 10/10/2019

Importancia: Crítica

Recursos afectados:

Solarwinds Dameware Mini Remote Client Agent Service, versión 12.1.0.89.

Descripción:

Tenable ha encontrado una vulnerabilidad de severidad crítica. Un atacante remoto, sin autenticación, podría ejecutar código arbitrario en el dispositivo.

Solución:

Todavía no hay una solución disponible.

Detalle:

SolarWinds Dameware Remote Mini Remote Client Agent Service soporta por defecto la autenticación de tarjetas inteligentes, lo que permite al usuario cargar un ejecutable en el *host* DWRCS.exe. El ejecutable se guardará en *C:WindowsTemp* como *dwDrvInst.exe*, y se ejecutará con los privilegios de la cuenta del *Local System*. Un atacante remoto no autenticado puede solicitar el inicio de sesión de la tarjeta inteligente para cargar y ejecutar un archivo arbitrario bajo la cuenta del *Local System*. Se ha asignado el identificador CVE-2019-3980 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Juniper

Fecha de publicación: 10/10/2019

Importancia: Crítica

Recursos afectados:

- Junos OS 12.3X48, 15.1X49, 17.3, 17.4. Plataformas afectadas: SRX Series.
- Junos OS 18.1, 18.1X75, 18.2, 18.2X75, 18.3, 18.4. Plataformas afectadas: MX2008, MX2010, MX2020, MX480, MX960.
- Junos OS. Plataformas afectadas: NFX Series.
- Junos OS 12.3X48. Plataformas afectadas: SRX Series.
- Junos OS 18.1, 18.1X75.
- Junos OS 15.1X49, 18.2, 18.4. Plataformas afectadas: SRX Series.
- Junos OS 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4.
- Junos OS 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, 18.2, 18.3, 18.4, 19.1.
- Junos OS. Plataformas afectadas: SRX 5000 Series.
- Junos OS 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4. Plataformas afectadas: MX Series.
- Junos OS 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3.
- 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, 18.2, 18.3, 18.4.
- Junos OS 15.1X49, 17.4, 18.1, 18.2, 18.3, 18.4. Plataformas afectadas: SRX1500.
- Junos OS 12.3X48, 15.1X49, 17.4, 18.1, 18.2, 18.3. Plataformas afectadas: SRX Series.
- Junos OS. Plataformas afectadas: NFX Series.
- Junos OS 18.1R3-S4, 18.3R1-S3. Plataformas afectadas: EX2300, EX2300-C, EX3400.
- Contrail Networking.

Descripción:

Este aviso contiene múltiples vulnerabilidades en Junos OS y en Contrail Networking.

Solución:

Actualizar los productos afectados desde el centro de descargas de Juniper.

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas en Junos OS, podría llegar a realizar las siguientes acciones en los productos afectados:

- Denegación de servicio: se han asignado los identificadores CVE-2019-0055, CVE-2019-0056, CVE-2019-0059, CVE-2019-0060, CVE-2019-0064, CVE-2019-0065, CVE-2019-0066, CVE-2019-0050 y CVE-2019-0075 para estas vulnerabilidades.
- Evasión de autenticación: se ha asignado el identificador CVE-2019-0057 para esta vulnerabilidad.
- Escalada de privilegios: se han asignado los identificadores CVE-2019-0058, CVE-2019-0061, CVE-2019-0070 y CVE-2019-0071 para estas vulnerabilidades.

- Obtener acceso como administrador: se ha asignado el identificador CVE-2019-0062 para esta vulnerabilidad.
- Realizar acciones administrativas en el dispositivo Junos: se ha asignado el identificador CVE-2019-0047 para esta vulnerabilidad.

También se han resuelto múltiples vulnerabilidades del software de terceros utilizado en Juniper Networks Contrail Networking, en su versión 1910. Para más información, consulte la sección de *Referencias*.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de tipo XXE en múltiples productos de Dell EMC

Fecha de publicación: 11/10/2019

Importancia: Alta

Recursos afectados:

- Dell EMC Avamar Server, versiones 7.4.1, 7.5.0, 7.5.1, 18.2 y 19.1;
- Dell EMC Integrated Data Protection Appliance (IDPA), versiones 2.0, 2.1, 2.2, 2.3 y 2.4.

Descripción:

Múltiples productos de Dell EMC contienen una vulnerabilidad, clasificada con severidad alta, de inyección de Entidad Externa XML (*XXE*).

Solución:

Dell recomienda aplicar distintos *hotfix*, según la versión de los productos afectados:

- Dell EMC Avamar Server:
  - 7.4.1;
  - 7.5.0;
  - 7.5.1;
  - 18.2;
  - 19.1.
- Dell EMC Integrated Data Protection Appliance (IDPA):
  - 2.0;
  - 2.1;
  - 2.2;
  - 2.3;
  - 2.4.

Detalle:

La vulnerabilidad de tipo XXE permitiría que un atacante remoto, no autenticado, generara una condición de denegación de servicio (DoS) o una exposición de información al proporcionar definiciones de tipo de documento (DTD), especialmente diseñadas en una solicitud XML. Se ha reservado el identificador CVE-2019-3752 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Evasión de restricciones de Runas en sudo

Fecha de publicación: 15/10/2019

Importancia: Alta

Recursos afectados:

Sudo, versiones anteriores a la 1.8.28.

Descripción:

Una vulnerabildiad de criticidad alta en *sudo* podría permitir a un atacante evadir las restricciones *Runas* y ejecutar comandos como *root*.

Solución:

Actualizar a la versión 1.8.28.

Detalle:

Cuando *sudo* es configurado para permitir a los usuarios ejecutar comandos arbitrarios mediante el parámetro *ALL* en *Runas*, es posible ejecutar comandos como *root* empleando los ID de usuario -1 o 4294967295. Un atacante local, autenticado, con privilegios de *sudo*, podría ejecutar comandos como *root* evadiendo las restricciones de usuario de *Runas* en el sistema. Se ha reservado el identificador CVE-2019-14287 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Actualización de seguridad 5.2.4 para WordPress

Fecha de publicación: 15/10/2019

Importancia: Media

Recursos afectados:

WordPress, versiones 5.2.3 y anteriores.

Descripción:

Se ha publicado la última versión de WordPress, que corrige 6 problemas de seguridad.

Solución:

- Actualizar a la versión 5.2.4.
- Las versiones actualizadas de WordPress 5.1 y anteriores también están disponibles para cualquier usuario que aún no haya actualizado a la versión 5.2.

Detalle:

Las correcciones de seguridad solucionan las siguientes vulnerabilidades que podrían permitir a un atacante:

- realizar ataques *Cross-Site Scripting* (XSS) a través de Customizer.
- ver los mensajes no autenticados.
- inyectar código Javascript en etiquetas de estilo a través de Stored Cross-Site Scripting.
- envenenamiento de caché de las peticiones de JSON GET a través de Vary.
- falsificar peticiones en el lado del servidor en la forma en que se validan las URLs.

Etiquetas: Actualización, CMS, Vulnerabilidad

Actualizaciones críticas en Oracle (octubre 2019)

Fecha de publicación: 16/10/2019

Importancia: Crítica

Recursos afectados:

- Agile Recipe Management para Pharmaceuticals, versiones 9.3.3 y 9.3.4;
- Diagnostic Assistant, versión 2.12.36;
- Enterprise Manager Base Platparam, versiones 13.2 y 13.3;
- Enterprise Manager para Exadata, versiones 12.1.0.5.0, 13.2.2.0.0, 13.3.1.0.0 y 13.3.2.0.0;
- Enterprise Manager Ops Center, versiones 12.3.3 y 12.4.0;
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versiones anteriores a XCP2361 y anteriores a XCP3071;
- Hyperion Data Relationship Management, versión 11.1.2.4;
- Hyperion Enterprise Perparamance Management Architect, versión 11.1.2.4;
- Hyperion Financial Reporting, versión 11.1.2.4;
- Instantis EnterpriseTrack, versiones 17.1, 17.2 y 17.3;
- JD Edwards EnterpriseOne Tools, versión 4.0.1.0;
- MICROS Relate CRM Software, versiones 7.1.0, 11.4, 15.0.0, 16.0.0, 17.0.0 y 18.0.0;
- MICROS Retail XBRi Loss Prevention, versión 10.8.3;
- MySQL Connectors, versiones 5.3.13 y anteriores, 8.0.17 y anteriores;
- MySQL Enterprise Monitor, versiones 8.0.17 y anteriores;
- MySQL Server, versiones 5.6.45 y anteriores, 5.7.27 y anteriores, 8.17 y anteriores;
- MySQL Workbench, versiones 8.0.17 y anteriores;
- Oracle Agile PLM, versiones 9.3.3-9.3.6;
- Oracle Agile Product Lifecycle Management para Process, versiones 6.2.0.0, 6.2.1.0, 6.2.2.0 y 6.2.3.0;
- Oracle API Gateway, versión 11.1.2.4.0;
- Oracle Application Testing Suite, versiones 13.2 y 13.3;
- Oracle Banking Digital Experience, versiones 18.1, 18.2, 18.3 y 19.1;
- Oracle Banking Platparam, versiones 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.7.0 y 2.7.1;
- 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 Clusterware, versión 19.0.0.0.0;
- Oracle Data Integrator, versión 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 12.1.1-12.1.3 y 12.2.3-12.2.9;
- Oracle Enterprise Repository, versión 12.1.3.0.0;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 8.0.2-8.0.8;
- Oracle Financial Services Enterprise Financial Perparamance Analytics, versiones 8.0.6 y 8.0.7;
- Oracle Financial Services Retail Perparamance Analytics, versiones 8.0.6 y 8.0.7;
- Oracle FLEXCUBE Direct Banking, versiones 12.0.2 y 12.0.3;
- Oracle params, versión 12.2.1.3.0;
- Oracle GoldenGate Application Adapters, versión 12.3.2.1.0;
- Oracle GraalVM Enterprise Edition, versión 19.2.0;
- Oracle Healthcare Foundation, versiones 7.1.1 y 7.2.2;
- Oracle Healthcare Translational Research, versiones 3.1.0, 3.2.1 y 3.3.1;
- Oracle Hospitality Cruise Dining Room Management, versión 8.0.80;
- Oracle Hospitality Guest Access, versiones 4.2.0 y 4.2.1;
- Oracle Hospitality Materials Control, versión 18.1;
- Oracle Hospitality Reporting y Analytics, versión 9.1.0;
- Oracle Hospitality RES 3700, versión 5.7;
- Oracle Java SE, versiones 7u231, 8u221, 11.0.4 y 13;
- Oracle Java SE Embedded, versión 8u221;
- Oracle JDeveloper y ADF, versiones 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0 y 12.2.1.3.0;
- Oracle NoSQL Database, versiones anteriores a 19.3.12;
- Oracle Outside In Technology, versión 8.5.4;
- Oracle Policy Automation, versiones 10.4.7, 12.1.0, 12.1.1 y 12.2.0-12.2.15;
- Oracle Policy Automation Connector para Siebel, versión 10.4.6;
- Oracle Policy Automation para Mobile Devices, versiones 12.2.0-12.2.15;
- Oracle Retail Customer Insights, versiones 15.0 y 16.0;
- Oracle Retail Customer Management y Segmentation Foundation, versión 17.0;
- Oracle Retail Integration Bus, versiones 15.0 y 16.0;
- Oracle Retail Xstore Office, versión 7.1;
- Oracle Retail Xstore Point of Service, versiones 7.1, 15.0, 16.0, 17.0, 17.0.3, 18.0, 18.0.1 y 19.0.0;

- Oracle Service Bus, versiones 11.1.1.9.0, 12.1.3.0.0 y 12.2.1.3.0;
- Oracle SOA Suite, versión 12.2.1.3.0;
- Oracle Solaris, versiones 10 y 11;
- Oracle Virtual Directory, versión 11.1.1.9.0;
- Oracle VM VirtualBox, versiones anteriores a 5.2.34 y anteriores a 6.0.14;
- Oracle Web Services, versión 12.2.1.3.0;
- Oracle WebCenter Portal, 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;
- PeopleSoft Enterprise HCM Human Resources, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56 y 8.57;
- PeopleSoft Enterprise SCM eProcurement, versión 9.2;
- Primavera Gateway, versiones 15.2, 16.2, 17.12 y 18.8;
- Primavera P6 Enterprise Project Portfolio Management, versiones 15.1.0-15.2.18, 16.1.0-16.2.18, 17.1.0-17.12.14 y 18.1.0-18.8.13;
- Primavera Unifier, versiones 16.1, 16.2, 17.7-17.12 y 18.8;
- Siebel Applications, versiones 19.8 y anteriores.

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 219 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, Java, Oracle, Virtualización, Vulnerabilidad

---

Vulnerabilidad en Workload Scheduler de IBM

Fecha de publicación: 16/10/2019

Importancia: Alta

Recursos afectados:

- Tivoli Workload Scheduler Distributed, versión 9.2.0 FP03 y anteriores.
- IBM Workload Scheduler Distributed:
  - versión 9.3.0 FP03 y anteriores,
  - versión 9.4.0 FP05 y anteriores,
  - versión 9.5.0 GA.

Descripción:

Davide Cioccia, ingeniero senior de seguridad en ING, ha detectado la vulnerabilidad de criticidad alta. Un atacante local podría modificar ficheros u obtener privilegios de *root* en el sistema.

Solución:

IBM ha publicado actualizaciones en función de las versiones, productos y plataformas afectadas. Pueden descargarse a través de su centro de descarga de software.

Detalle:

La vulnerabilidad se debe a la posibilidad, por parte de un usuario local, de escribir archivos como *root* en el sistema de archivos. Un atacante local podría modificar ficheros u obtener privilegios de *root* en el sistema. Se ha reservado el identificador CVE-2019-4031 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Control de acceso inadecuado en productos VMware

Fecha de publicación: 16/10/2019

Importancia: Crítica

Recursos afectados:

- VMware Cloud Foundation,
- VMware Harbor Container Registry para PCF, versiones 1.8.X.

Descripción:

Se ha publicado una vulnerabilidad de control de acceso inadecuado en direcciones PCF rotas en los productos VMware indicados.

Solución:

- Para VMware Cloud Foundation, el parche que corrige la vulnerabilidad se publicará próximamente.
- Para VMware Harbor Container Registry para PCF, aplicar el parche 1.8.4

Detalle:

Una vulnerabilidad del control de acceso roto podría permitir a un atacante, con acceso administrativo a un proyecto, crear una cuenta robot dentro de un proyecto adyacente a través de la API de Harbor. Esto podría conducir a un acceso no autorizado para insertar, extraer o modificar imágenes en el proyecto adyacente de destino. Se ha reservado el identificador CVE-2019-16919 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 17/10/2019

Importancia: Crítica

Recursos afectados:

- Prodcutos de Cisco que estén ejecutando una versión vulnerable de:
  - Aironet 1540 Series APs,
  - Aironet 1560 Series APs,
  - Aironet 1800 Series APs,
  - Aironet 1810 Series APs,
  - Aironet 1830 Series APs,
  - Aironet 1850 Series APs,
  - Aironet 2800 Series APs,
  - Aironet 3800 Series APs,
  - Aironet 4800 APs,
  - Catalyst 9100 APs (la versión 8.9.100.0 es la primera versión soportada).
- Cisco WLC Software, versión 8.5.140.0 y anteriores;
- Cisco SPA112 2-Port Phone Adapter y SPA122 ATA con Router, versión de *firmware* 1.4.1 SR4 y anteriores, con la interfaz de gestión basada en web habilitada;
- Cisco 250 Series Smart Switches;
- Cisco 350 Series Managed Switches;
- Cisco 550X Series Stackable Managed Switches.

Descripción:

Cisco ha publicado 18 vulnerabilidades, 1 de severidad crítica y 17 de severidad alta, que afectan a sus productos.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

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

- acceso no autorizado al dispositivo con privilegios elevados;
- denegación remota del servicio;
- ejecución remota de código;
- ejecución remota de ataques de CSRF (*Cross-Site Request Forgery*).

Para estas vulnerabilidades, se han asignado los siguientes identificadores: CVE-2019-15260, CVE-2019-15262, CVE-2019-15240, CVE-2019-15241, CVE-2019-15242, CVE-2019-15243, CVE-2019-15244, CVE-2019-15245, CVE-2019-15246, CVE-2019-15247, CVE-2019-15248, CVE-2019-15249, CVE-2019-15250, CVE-2019-15251, CVE-2019-15252, CVE-2019-12636, CVE-2019-15261 y CVE-2019-15264.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Autenticación incorrecta en múltiples dispositivos de ABB.

Fecha de publicación: 18/10/2019

Importancia: Baja

Recursos afectados:

- UNO-DM, versión 1.8.2 y anteriores;
- PVS-100-TL y PVS120-TL, versión 0.10.14 y anteriores;
- PVS-175-TL, versión 0.2.6 y anteriores;
- PVS-50/60 y TRIO-TM, versión 1.2.15 y anteriores;
- REACT 2, versión 0.2.19 y anteriores.

Descripción:

El investigador Maxim Rupp ha reportado una vulnerabilidad de autenticación incorrecta que podría permitir a un atacante tener acceso a la información de los productos afectados sin necesidad de autenticarse.

Solución:

Actualizar a las siguientes versiones:

- UNO-DM versión 1.8.3.
- PVS-100-TL y PVS120-TL versión 0.10.15.
- PVS-175-TL versión 0.2.7.
- PVS-50/60 y TRIO-TM versión 1.2.16.
- REACT 2 versión 0.2.20.

Detalle:

La vulnerabilidad de tipo autenticación incorrecta podría permitir que el producto tuviera acceso a cierta información en modo lectura sin la necesidad de realizar un proceso de autenticación previo. No se ha asignado identificador para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en FortiMail de Fortinet

Fecha de publicación: 21/10/2019

Importancia: Alta

Recursos afectados:

- FortiMail, versiones:
  - 6.2.0,
  - 6.0.0 hasta 6.0.6,
  - 5.4.10 y anteriores.

Descripción:

Fortinet ha descubierto dos vulnerabilidades con criticidades altas en FortiMail. Un atacante, con privilegios de administración, podría obtener acceso no autorizado al sistema.

Solución:

- Actualizar a las versiones de FortiMail:
  - 6.2.1,
  - 6.0.7,
  - 5.4.11. (pendiente de publicación).

Detalle:

- Ambas vulnerabildades se encuentran en la interfaz de usuario web de administración, pudiendo permitir a los administradores la realización de acciones a las que no estarían autorizados:
  - Un atacante, con privilegios de administrador, podría obtener acceso no autorizado a la consola web. Se ha reservado el identificador CVE-2019-15712 para esta vulnerabilidad.
  - Un atacante, con privilegios de administrador, podría obtener acceso no autorizado y descargar la configuración de la copia de seguridad del sistema. Se ha reservado el identificador CVE-2019-15707 para esta vulnerabilidad

Etiquetas: Actualización, Vulnerabilidad

Evasión de autentificación en Citrix Application Delivery Controller y Citrix Gateway

Fecha de publicación: 21/10/2019

Importancia: Alta

Recursos afectados:

- Citrix ADC y Citrix Gateway versión 13.0, hasta la build 41.20;
- Citrix ADC y NetScaler Gateway versión 12.1, hasta la build 54.13;
- Citrix ADC y NetScaler Gateway versión 12.0, hasta la build 62.8;
- Citrix ADC y NetScaler Gateway version 11.1, hasta la build 62.8;
- Citrix ADC y NetScaler Gateway version 10.5, hasta la build 70.5.

Descripción:

Se ha identificado una vulnerabilidad en la interfaz de gestión de Citrix Application Delivery Controller (ADC), anteriormente conocida como NetScaler ADC, y Citrix Gateway, anteriormente conocida como NetScaler Gateway.

Solución:

Actualizar a las siguientes versiones:

- Citrix ADC and Citrix Gateway versión 13.0, build 41.28 y posteriores;
- Citrix ADC and NetScaler Gateway versión 12.1, build 54.16 y posteriores;
- Citrix ADC and NetScaler Gateway versión 12.0, build 62.10 y posteriores;
- Citrix ADC and NetScaler Gateway versión 11.1, build 63.9 y posteriores;
- Citrix ADC and NetScaler Gateway versión 10.5, build 70.8 y posteriores.

Detalle:

Una vulnerabilidad en la interfaz de administración de los productos afectados podría permitir a un atacante, que tenga acceso a ella, obtener acceso al dispositivo con permisos de administrador.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en Security Access Manager de IBM

Fecha de publicación: 25/10/2019

Importancia: Alta

Recursos afectados:

Todas las versiones de IBM Security Access Manager.

Descripción:

Lczap, investigador de seguridad, ha reportado a IBM una vulnerabilidad de criticidad alta. Un atacante, sin autenticar, podría generar una condición de denegación de servicio.

Solución:

Por el momento, no se dispone de actualización que solucione la vulnerabilidad. IBM ha publicado unas indicaciones para mitigar este tipo de ataques.

Detalle:

IBM Security Access Manager es vulnerable a ataques del tipo Slow HTTP Attack. Un atacante, sin autenticación, podría generar una condición de denegación de servicio en el sistema. Se ha reservado el identificador CVE-2019-4036 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Múltiples vulnerabilidades en RouterOS de MikroTik

Fecha de publicación: 29/10/2019

Importancia: Alta

Recursos afectados:

- RouterOS Stable, con versiones 6.45.6 y anteriores,
- RouterOS Long-term, con versiones 6.44.5 y anteriores.

Descripción:

Jacob Baines, investigador de seguridad en Tenable, ha descubierto 4 vulnerabilidades con criticidades altas. Un atacante remoto, no autenticado, podría acceder, modificar u obtener privilegios de *root* en el dispositivo.

Solución:

- MikroTik ha publicado actualizaciones que solucionan las vulnerabilidades:
  - RouterOS Stable, actualizar a la versión 6.45.7,
  - RouterOS Long-term, actualizar a la versión 6.44.6.

Detalle:

- Una vulnerabilidad se encuentra en la posibilidad de realizar peticiones DNS al puerto 8291. Un atacante remoto, no autenticado, podría realizar un ataque de envenenamiento de cache DNS en el dispositivo. Se ha asignado el identificador CVE-2019-3978 para esta vulnerabilidad.
- Una vulnerabilidad se debe al manejo indebido de repuestas DNS. Un atacante remoto, a través de un servidor DNS comprometido, podría enviar peticiones maliciosas para envenenar la caché DNS del router. Se ha asignado el identificador CVE-2019-3979 para esta vulnerabilidad.
- Una vulnerabilidad reside en el campo de nombre de los paquetes de actualizaciones. Un atacante podría generar un paquete de actualización malicioso, que si un usuario autenticado instalase en el dispositivo, podría habilitar un terminal con privilegios de *root*. Se ha asignado el identificador CVE-2019-3976 para esta vulnerabilidad.
- Una vulnerabilidad se encuentra en la falta de validación de paquetes de actualizaciones cuando el parámetro de autoactualizar se encuentra activo. Un atacante remoto podría realizar un *downgrade* del *firmware* del router y reiniciar los usuarios y contraseñas. Se ha asignado el identificador CVE-2019-3977 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Denegación de servicio en RDesktop

Fecha de publicación: 31/10/2019

Importancia: Alta

Recursos afectados:

RDesktop, anterior a la versión 1.8.4.

Descripción:

El investigador de seguridad, Pavel Cheremushkin, de Kaspersky ICS CERT ha detectado una vulnerabilidad en RDesktop, que podría permitir a un atacante remoto generar una condición de denegación de servicio.

Solución:

Actualizar a la versión 1.8.5.

Detalle:

Múltiples vulnerabilidades de lectura fuera de límites podrían permitir a un atacante provocar la denegación de servicio (DoS).

Etiquetas: Actualización, Vulnerabilidad