Boletín de julio de 2020

Avisos Técnicos

Vulnerabilidad de ejecución remota de código en TMUI de F5

Fecha de publicación: 01/07/2020

Importancia: Crítica

Recursos afectados:

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.1.0 y 15.0.0;
- desde 14.1.0 hasta 14.1.2;
- desde 13.1.0 hasta 13.1.3;
- desde 12.1.0 hasta 12.1.5;
- desde 11.6.1 hasta 11.6.5.

Descripción:

Mikhail Klyuchnikov, de Positive Technologies, notificó a F5 una vulnerabilidad, de severidad crítica, de tipo ejecución remota de código, que afecta a TMUI (*Traffic Management User Interface*) de F5.

Solución:

Actualizar los productos afectados a alguna de las siguientes versiones:

- 15.1.0.4;
- 14.1.2.6;
- 13.1.3.4;
- 12.1.5.2;
- 11.6.5.2.

Detalle:

Esta vulnerabilidad podría permitir a un atacante, independientemente de si está o no autenticado, con acceso de red a TMUI (también conocido como utilidad de configuración), a través del puerto de administración BIG-IP y/o Self IPs, ejecutar comandos arbitrarios del sistema, crear o eliminar archivos, deshabilitar servicios y/o ejecutar código Java arbitrariamente, lo que podría resultar en un compromiso completo del sistema. Se ha reservado el identificador CVE-2020-5902 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades de RCE en Microsoft Windows Codecs Library

Fecha de publicación: 02/07/2020

Importancia: Crítica

Recursos afectados:

Microsoft Windows Codecs Library en distintas versiones de Windows 10, solo los clientes que hayan instalado los códecs multimedia HEVC (incluidos los del fabricante del dispositivo) opcionales de Microsoft Store.

Descripción:

Abdul-Aziz Hariri, perteneciente a Zero Day Initiative de Trend Micro, ha reportado dos vulnerabilidades a Microsoft, una con severidad crítica y otra alta, ambas de tipo ejecución remota de código (RCE), que afectan a Microsoft Windows Codecs Library.

Solución:

Las versiones que solucionan estas vulnerabilidades son 1.0.31822.0, 1.0.31823.0 y posteriores.

Los clientes afectados serán actualizados automáticamente por Microsoft Store y no necesitan realizar ninguna acción para recibir la actualización, únicamente asegurarse de que tienen activada la funcionalidad de actualizaciones automáticas.

Alternativamente, los clientes que desean recibir la actualización de inmediato pueden buscar actualizaciones con la aplicación Microsoft Store.

Detalle:

- Existe una vulnerabilidad de ejecución remota de código (RCE) en la forma en que Microsoft Windows Codecs Library gestiona los objetos en la memoria. La explotación de la vulnerabilidad requiere que un programa procese un archivo de imagen especialmente diseñado. Un atacante podría obtener información para comprometer aún más el sistema del usuario. Se ha reservado el identificador CVE-2020-1425 para esta vulnerabilidad.
- Existe una vulnerabilidad de ejecución remota de código (RCE) en la forma en que Microsoft Windows Codecs Library gestiona los objetos en la memoria, que permitiría a un atacante ejecutar código arbitrario. La explotación de la vulnerabilidad requiere que un programa procese un archivo de imagen especialmente diseñado. Se ha reservado el identificador CVE-2020-1457 para esta vulnerabilidad.

Etiquetas: Actualización, Microsoft, Vulnerabilidad, Windows

Múltiples vulnerabilidades en productos de Citrix

Fecha de publicación: 08/07/2020

Importancia: Crítica

Recursos afectados:

- Citrix ADC y Citrix Gateway, anteriores a 13.0-58.30;
- Citrix ADC y NetScaler Gateway, anteriores a 12.1-57.18;
- Citrix ADC y NetScaler Gateway, anteriores a 12.0-63.21;
- Citrix ADC y NetScaler Gateway, anteriores a 11.1-64.14;
- NetScaler ADC y NetScaler Gateway, anteriores a 10.5-70.18;
- Citrix SD-WAN WANOP, anteriores a 11.1.1ay;
- Citrix SD-WAN WANOP, anteriores a 11.0.3d;
- Citrix SD-WAN WANOP, anteriores a 10.2.7;
- Citrix Gateway Plug-in para Linux, anteriores a 1.0.0.137.

Descripción:

Citrix ha informado de múltiples vulnerabilidades en productos Citrix ADC?(conocidos como NetScaler ADC), Citrix Gateway?(conocidos como NetScaler Gateway)?y Citrix SD-WAN WANOP que podría permitir a un atacante realizar ataques de denegación de servicio, inyecciones de código, elevación de privilegios, divulgación de información, o Cross Site Scripting (XSS).

Solución:

Citrix ha publicado versiones para Citrix ADC, Citrix Gateway y Citrix SD-WAN WANOP que solucionan estas vulnerabilidades. Citrix recomienda encarecidamente que los clientes instalen inmediatamente estas actualizaciones.

Detalle:

Las vulnerabilidades reportadas por Citrix permiten comprometer los sistemas afectados, efectuar un ataque Cross Site Scripting (XSS) en el interfaz administrativo o generar una descarga para el dispositivo que podría comprometer el equipo local del usuario si es ejecutado desde la red de administración, así como ataques de denegación de servicio o elevación de privilegios.

Para estas vulnerabilidades se han asignado los identificadores: CVE-2019-18177, CVE-2020-8187, CVE-2020-8190, CVE-2020-8191, CVE-2020-8193, CVE-2020-8194, CVE-2020-8195, CVE-2020-8196, CVE-2020-8197, CVE-2020-8198 y CVE-2020-8199.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Xen

Fecha de publicación: 08/07/2020

Importancia: Alta

Recursos afectados:

Todas las versiones de Xen son vulnerables.

Descripción:

Diversos investigadores han detectado 5 vulnerabilidades, que en su conjunto afectan a todas las versiones de Xen.

Solución:

Aplicar los correspondientes parches que aparecen listados en la sección *RESOLUTION* de cada aviso de Xen, disponibles en las *Referencias*.

Detalle:

- Cuando el administrador configura un invitado (*guest*) para permitir más de 1023 canales de eventos, ese invitado puede bloquear

el *host*. Cuando Xen se queda sin memoria, la asignación de nuevos canales de eventos provocará el bloqueo del *host* en lugar de informar con un error. Se ha asignado el identificador CVE-2020-15566 para esta vulnerabilidad.
- Un invitado de HVM malintencionado podría hacer que el hipervisor se bloquee, lo que generaría una condición de denegación de servicio (DoS) que afectaría a todo el *host*. Se ha asignado el identificador CVE-2020-15563 para esta vulnerabilidad.
- Un invitado malintencionado podría retener el acceso de lectura/escritura de DMA a los *frames* devueltos al *pool* de Xen y luego reutilizarlos para otro propósito, lo que podría causar bloqueos del *host* (que conducirían a una denegación de servicio) y una escalada de privilegios. Se ha asignado el identificador CVE-2020-15565 para esta vulnerabilidad.
- Un administrador invitado, malintencionado, podría causar un bloqueo del hipervisor, lo que resultaría en una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-15564 para esta vulnerabilidad.
- Un administrador invitado, e incluso un usuario invitado no privilegiado, podrían causar condiciones de denegación de servicio, corrupción de datos o escalada de privilegios. Se ha asignado el identificador CVE-2020-15567 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Junos Space y Junos OS de Juniper

Fecha de publicación: 09/07/2020

Importancia: Crítica

Recursos afectados:

- Junos OS en la plataforma SRX Series, versiones 18.1, 18.2, 18.3, 18.4, 19.1, 19.2 y 19.3;
- Junos Space Security Director de Junos Space, versiones anteriores a 20.1R1.

Descripción:

Juniper ha informado de varias vulnerabilidades en sus productos Junos OS y Junos Space Security Director, que permitirían a un atacante ejecutar código remoto en los sistemas o provocar una condición de denegación de servicio.

Solución:

- Actualizar Junos OS a las versiones 18.1R3-S9, 18.2R2-S7, 18.2R3-S3, 18.3R1-S7, 18.3R2-S4, 18.3R3-S1, 18.4R1-S7, 18.4R2 -S4, 18.4R3, 19.1R1-S5, 19.1R2, 19.2R1-S2, 19.2R2, 19.3R2 o 19.4R1;
- actualizar Junos Space Security Director a la versión 20.1R1.

Detalle:

Las vulnerabilidades encontradas en Junos OS se producen en el servicio de redireccionamiento ICAP por un procesamiento inadecuado de un mensaje HTTP o por fallo en la gestión de datos en la memoria. Estas vulnerabilidades, calificadas como críticas, solo son efectivas cuando el servicio ICAP está habilitado.

En cuanto a las vulnerabilidades encontradas en Junos Space Security Director, Juniper ha corregido un total de 105 vulnerabilidades en la versión publicada 20.1R1, siendo 18 de ellas calificadas como críticas.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de inyección de comandos en IBM QRadar SIEM

Fecha de publicación: 14/07/2020

Importancia: Crítica

Recursos afectados:

IBM QRadar SIEM, versiones:

- desde 7.4.0, hasta 7.4.0 Patch 2;
- desde 7.3.0, hasta 7.3.3 Patch 3.

Descripción:

Se ha identificado una vulnerabilidad, de severidad crítica, que afecta a varias versiones de IBM QRadar SIEM.

Solución:

Actualizar el producto afectado a las versiones 7.4.0 Patch 3 o 7.3.3 Patch 4 para solucionar la vulnerabilidad indicada.

Detalle:

IBM QRadar SIEM podría permitir que un usuario privilegiado, remoto, ejecutase comandos. Se ha reservado el identificador CVE-2020-4512 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de julio de 2020

Fecha de publicación: 15/07/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows,
- Microsoft Edge (basado en EdgeHTML),
- Microsoft Edge (basado en Chromium) en modo IE,
- Microsoft ChakraCore,
- Internet Explorer,
- Microsoft Office, Microsoft Office Services y Web Apps,
- Windows Defender,
- Skype para Business,
- Visual Studio,
- Microsoft OneDrive,
- Open Source Software,
- .NET Framework,
- Azure DevOps.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de julio, consta de 115 vulnerabilidades, 12 clasificadas como críticas y 103 como importantes.

Solución:

- Instalar la actualización de seguridad correspondiente. En la página de Microsoft se informa de los distintos métodos para llevar a cabo dichas actualizaciones.
- **IMPORTANTE:** Microsoft destaca una vulnerabilidad de ejecución remota de código (RCE) que afecta a Windows Domain Name System (DNS) Server. La siguiente modificación del registro se ha identificado como una solución para esta vulnerabilidad (es necesario reiniciar el servicio DNS para que surta efecto):

```
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesDNSParameters
DWORD = TcpReceivePacketSize
Value = 0xFF00
```

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- ejecución remota de código,
- escalada de privilegios,
- denegación de servicio,
- divulgación de información,
- suplantación de identidad (*spoofing*).

IMPORTANTE: Existe una vulnerabilidad de ejecución remota de código (RCE) en los servidores de Windows Domain Name System (DNS) cuando no pueden gestionar correctamente las solicitudes. Un atacante podría enviar solicitudes maliciosas a un servidor DNS de Windows, lo que le permitiría ejecutar código arbitrario en el contexto de la cuenta del sistema local. Los servidores de Windows que están configurados como servidores DNS están expuestos a esta vulnerabilidad. Esta vulnerabilidad es susceptible de aprovecharse de forma masiva. Se ha asignado el identificador CVE-2020-1350 para esta vulnerabilidad.

Etiquetas: Actualización, DNS, Microsoft, Navegador, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en Apache Tomcat

Fecha de publicación: 15/07/2020

Importancia: Crítica

Recursos afectados:

Apache Tomcat, versiones:

- desde la 7.0.27, hasta la 7.0.104;
- desde la 8.5.0, hasta la 8.5.56;
- desde la 9.0.0.M1, hasta la 9.0.36;
- desde la 10.0.0-M1, hasta la 10.0.0-M6.

Descripción:

Las versiones 7, 8, 9 y 10 de Apache Tomcat están afectadas por 2 vulnerabilidades, una severidad crítica y otra media, de tipo denegación de servicio (DoS) en WebSocket y DoS en el protocolo HTTP/2, respectivamente.

Solución:

Actualizar a las versiones:

- 7.0.105;
- 8.5.57;
- 9.0.37;
- 10.0.0-M7.

Detalle:

- La longitud del *payload* en un marco de WebSocket no se valida correctamente. Las longitudes de *payload* no válidas podrían desencadenar un bucle infinito. Múltiples solicitudes con longitudes de carga no válidas podrían conducir a una denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-13935 para esta vulnerabilidad.
- Una conexión directa h2c (HTTP/2 sobre TCP) no libera el procesador HTTP/1.1 después de la actualización a HTTP/2. Si se hiciera un número suficiente de tales solicitudes, podría producirse una excepción *OutOfMemoryException* que llevaría a una denegación de servicio (DoS). No afecta a la versión 7 de Apache Tomcat. Se ha asignado el identificador CVE-2020-13934 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Actualizaciones críticas en Oracle (julio 2020)

Fecha de publicación: 15/07/2020

Importancia: Crítica

Recursos afectados:

- Category Management Planning & Optimization, versión 15.0.3;
- Customer Management y Segmentation Foundation, versiones 16.0, 17.0, 18.0;
- Enterprise Manager Base Platform, versiones 12.1.0.5, 13.3.0.0, 13.4.0.0;
- Enterprise Manager for Fusion Middleware, versión 12.1.0.5;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- GoldenGate Stream Analytics, versiones anteriores a 19.1.0.0.1;
- Hyperion Financial Close Management, versión 11.1.2.4;
- Instantis EnterpriseTrack, versiones 17.1-17.3;
- JD Edwards EnterpriseOne Orchestrator, versiones anteriores a 9.2.4.2;
- JD Edwards EnterpriseOne Tools, versiones anteriores a 9.2.3.3, anteriores a 9.2.4.2;
- MySQL Client, versiones 5.6.48 y anteriores, 5.7.30 y anteriores, 8.0.20 y anteriores;
- MySQL Cluster, versiones 7.3.29 y anteriores, 7.4.28 y anteriores, 7.5.18 y anteriores, 7.6.14 y anteriores, 8.0.20 y anteriores;
- MySQL Connectors, versiones 8.0.20 y anteriores;
- MySQL Enterprise Monitor, versiones 4.0.12 y anteriores, 8.0.20 y anteriores;
- MySQL Server, versiones 5.6.48 y anteriores, 5.7.30 y anteriores, 8.0.20 y anteriores;
- Oracle Agile Engineering Data Management, versión 6.2.1.0;
- Oracle Application Express, versiones 5.1-19.2;
- Oracle Application Testing Suite, versiones 13.2.0.1, 13.3.0.1;
- Oracle AutoVue, versión 21.0;
- Oracle Banking Enterprise Collections, versiones 2.7.0-2.9.0;
- Oracle Banking Payments, versiones 14.1.0-14.4.0;
- Oracle Banking Platform, versiones 2.4.0-2.10.0;
- Oracle Berkeley DB, versiones anteriores a 6.1.38, anteriores a 18.1.40;
- Oracle BI Publisher, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Business Process Management Suite, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Coherence, versiones 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0;
- Oracle Commerce Guided Search / Oracle Commerce Experience Manager, versiones 11.0, 11.1, 11.2, anteriores a 11.3.1;
- Oracle Commerce Platform, versiones 11.1, 11.2, anteriores a 11.3.1;
- Oracle Commerce Service Center, versiones 11.1, 11.2, anteriores a 11.3.1;
- Oracle Communications Analytics, versión 12.1.1;
- Oracle Communications Billing y Revenue Management, versiones 7.5.0.23.0, 12.0.0.3.0;
- Oracle Communications BRM - Elastic Charging Engine, versiones 11.3, 12.0;
- Oracle Communications Contacts Server, versión 8.0.0.4.0;
- Oracle Communications Convergence, versiones 3.0.1.0-3.0.2.1;
- Oracle Communications Diameter Signaling Router (DSR), versiones 8.0-8.4;
- Oracle Communications Element Manager, versiones 8.1.1, 8.2.0, 8.2.1;
- Oracle Communications Evolved Communications Application Server, versión 7.1;
- Oracle Communications Instant Messaging Server, versión 10.0.1.4.0;
- Oracle Communications Interactive Session Recorder, versiones 6.1-6.4;
- Oracle Communications IP Service Activator, versiones 7.3.0, 7.4.0;
- Oracle Communications LSMS, versiones 13.0-13.3;
- Oracle Communications Messaging Server, versiones 8.0.2, 8.1.0;
- Oracle Communications MetaSolv Solution, versión 6.3.0;
- Oracle Communications Network Charging y Control, versiones 6.0.1, 12.0.0-12.0.3;
- Oracle Communications Network Integrity, versiones 7.3.2-7.3.6;
- Oracle Communications Operations Monitor, versiones 3.4, 4.1-4.3;
- Oracle Communications Order y Service Management, versiones 7.3, 7.4;
- Oracle Communications Services Gatekeeper, versiones 6.0, 6.1, 7.0;
- Oracle Communications Session Border Controller, versiones 8.1.0, 8.2.0, 8.3.0;
- Oracle Communications Session Report Manager, versiones 8.1.1, 8.2.0, 8.2.1;
- Oracle Communications Session Route Manager, versiones 8.1.1, 8.2.0, 8.2.1;
- Oracle Configuration Manager, versión 12.1.2.0.6;
- Oracle Configurator, versiones 12.1, 12.2;
- Oracle Data Masking y Subsetting, versiones 13.3.0.0, 13.4.0.0;
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c, [Spatial Studio] anteriores a 19.2.1;
- Oracle E-Business Suite, versiones 12.1.1-12.1.3, 12.2.3-12.2.9;
- Oracle Endeca Information Discovery Studio, versión 3.2.0;
- Oracle Enterprise Communications Broker, versiones 3.0.0-3.2.0;
- Oracle Enterprise Repository, versión 11.1.1.7.0;
- Oracle Enterprise Session Border Controller, versiones 8.1.0, 8.2.0, 8.3.0;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 8.0.6-8.1.0;
- Oracle Financial Services Compliance Regulatory Reporting, versiones 8.0.6-8.0.8;
- Oracle Financial Services Lending y Leasing, versiones 12.5.0, 14.1.0-14.8.0;
- Oracle Financial Services Liquidity Risk Management, versión 8.0.6;
- Oracle Financial Services Loan Loss Forecasting y Provisioning, versiones 8.0.6-8.0.8;
- Oracle Financial Services Market Risk Measurement y Management, versiones 8.0.6, 8.0.8;
- Oracle Financial Services Regulatory Reporting for De Nederlysche Bank, versión 8.0.4;
- Oracle FLEXCUBE Investor Servicing, versiones 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0;
- Oracle FLEXCUBE Private Banking, versiones 12.0.0, 12.1.0;
- Oracle Fusion Middleware MapViewer, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Global Lifecycle Management/OPatch, versiones anteriores a 12.2.0.1.20;
- Oracle GoldenGate, versiones anteriores a 19.1.0.0.0;
- Oracle GraalVM Enterprise Edition, versiones 19.3.2, 20.1.0;
- Oracle Health Sciences Empirica Inspections, versión 1.0.1.2;
- Oracle Health Sciences Empirica Signal, versión 7.3.3;
- Oracle Healthcare Master Person Index, versión 4.0.2;
- Oracle Healthcare Translational Research, versiones 3.2.1, 3.3.1, 3.3.2, 3.4.0;
- Oracle Help Technologies, versiones 11.1.1.9.0, 12.2.1.3.0;

- Oracle Hospitality Guest Access, versiones 4.2.0, 4.2.1;
- Oracle Hospitality Reporting y Analytics, versión 9.1.0;
- Oracle Hyperion BI , versión 11.1.2.4;
- Oracle iLearning, versiones 6.1, 6.1.1;
- Oracle Insurance Accounting Analyzer, versiones 8.0.6-8.0.9;
- Oracle Insurance Data Gateway, versión 1.0;
- Oracle Insurance Policy Administration J2EE, versiones 10.2.0, 10.2.4, 11.0.2, 11.1.0, 11.2.0;
- Oracle Insurance Rules Palette, versiones 10.2.0, 10.2.4, 11.0.2, 11.1.0, 11.2.0;
- Oracle Java SE, versiones 7u261, 8u251, 11.0.7, 14.0.1;
- Oracle Java SE Embedded, versión 8u251;
- Oracle Outside In Technology, versiones 8.5.4, 8.5.5;
- Oracle Rapid Planning, versiones 12.1, 12.2;
- Oracle Real User Experience Insight, versión 13.3.1.0;
- Oracle Retail Assortment Planning, versiones 15.0, 15.0.3, 16.0, 16.0.3;
- Oracle Retail Bulk Data Integration, versiones 15.0, 16.0;
- Oracle Retail Customer Management y Segmentation Foundation, versión 18.0;
- Oracle Retail Data Extractor for Merchyising, versiones 1.9, 1.10, 18.0;
- Oracle Retail Extract Transform y Load, versión 19.0;
- Oracle Retail Financial Integration, versiones 15.0, 16.0;
- Oracle Retail Fusion Platform, versión 5.5;
- Oracle Retail Integration Bus, versiones 15.0, 15.0.3, 16.0, 16.0.3;
- Oracle Retail Invoice Matching, versión 16.0;
- Oracle Retail Item Planning, versión 15.0.3;
- Oracle Retail Macro Space Optimization, versión 15.0.3;
- Oracle Retail Merchyise Financial Planning, versión 15.0.3;
- Oracle Retail Merchyising System, versiones 15.0.3, 16.0.2, 16.0.3;
- Oracle Retail Order Broker, versión 15.0;
- Oracle Retail Predictive Application Server, versiones 14.0.3, 14.1.3, 15.0.3, 16.0.3;
- Oracle Retail Regular Price Optimization, versiones 15.0.3, 16.0.3;
- Oracle Retail Replenishment Optimization, versión 15.0.3;
- Oracle Retail Sales Audit, versión 14.1;
- Oracle Retail Service Backbone, versiones 14.1, 15.0, 16.0;
- Oracle Retail Size Profile Optimization, versión 15.0.3;
- Oracle Retail Store Inventory Management, versiones 14.0.4, 14.1.3, 15.0.3, 16.0.3;
- Oracle Retail Xstore Point of Service, versiones 7.1, 15.0, 16.0, 17.0, 18.0, 19.0;
- Oracle SD-WAN Aware, versión 8.2;
- Oracle SD-WAN Edge, versiones 8.2, 9.0;
- Oracle Security Service, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Solaris, versión 11;
- Oracle TimesTen In-Memory Database, versiones anteriores a 18.1.2.1.0;
- Oracle Transportation Management, versiones 6.3.7, 6.4.3;
- Oracle Unified Directory, versiones 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Utilities Framework, versiones 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0;
- Oracle VM VirtualBox, versiones anteriores a 5.2.44, anteriores a 6.0.24, anteriores a 6.1.12;
- Oracle WebCenter Portal, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle WebCenter Sites, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0;
- Oracle ZFS Storage Appliance Kit, versión 8.8;
- PeopleSoft Enterprise FIN Expenses, versión 9.2;
- PeopleSoft Enterprise HCM Global Payroll Switzerly, versión 9.2;
- PeopleSoft Enterprise HRMS, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57, 8.58;
- Primavera Gateway, versiones 16.2.0-16.2.11, 17.12.0-17.12.7, 18.8.0-18.8.9, 19.12.0-19.12.4;
- Primavera P6 Enterprise Project Portfolio Management, versiones 16.1.0.0-16.2.20.1, 17.1.0.0-17.12.17.1, 18.1.0.0-18.8.19, 19.12.0-19.12.6;
- Primavera Portfolio Management, versiones 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0, 19.0.0.0;
- Primavera Unifier, versiones 16.1, 16.2, 17.7-17.12, 18.8, 19.12, [Mobile App] anteriores a 20.6;
- Siebel Applications, versiones 2.20.5 y anteriores, 20.6 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 443 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

---

Actualización de seguridad de SAP de julio de 2020

Fecha de publicación: 15/07/2020

Importancia: Crítica

Recursos afectados:

- SAP NetWeaver, versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP Business Client, versión 6.5;
- SAP Disclosure Management, versión 1.0;
- SAP Business Objects Business Intelligence Platform, versiones 4.1 y 4.2.

Descripción:

SAP ha publicado varias actualizaciones de seguridad, que afectan a 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 8 notas de seguridad y 2 actualizaciones, siendo 2 de severidad crítica, 1 alta, 6 medias y 1 baja.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 4 vulnerabilidad de *Cross-Site Scripting*,
- 2 vulnerabilidades de divulgación de información,
- 1 vulnerabilidad de falta de autenticación,
- 1 vulnerabilidad de acceso a rutas no controlado (*path traversal*),
- 1 vulnerabilidad de SSRF (*Server Side Request Forgery*),
- 5 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- SAP NetWeaver AS JAVA (LM Configuration Wizard) no realiza una verificación de autenticación, lo que permitiría a un atacante, sin autenticación previa, ejecutar tareas de configuración para realizar acciones críticas contra el sistema SAP Java, incluida la capacidad de crear un usuario administrativo y, por lo tanto, comprometer la confidencialidad, integridad y disponibilidad del sistema. Se han asignado los identificadores CVE-2020-6287 y CVE-2020-6286 para esta vulnerabilidad.
- SAP NetWeaver - XML Toolkit para JAVA (ENGINEAPI), bajo ciertas condiciones, permitiría a un atacante acceder a información que de otro modo estaría restringida, lo que llevaría a una divulgación de información. Se ha asignado el identificador CVE-2020-6285 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-6267, CVE-2020-6289, CVE-2020-6290, CVE-2020-6291, CVE-2020-6292, CVE-2020-6281, CVE-2020-6276, CVE-2020-6282, CVE-2020-6278, CVE-2020-6222 y CVE-2020-6280.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.20

Fecha de publicación: 15/07/2020

Importancia: Baja

Recursos afectados:

Versiones de Joomla! de la 2.5.0 a la 3.9.19.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 6 vulnerabilidades, todas ellas de severidad baja, que afectan a su núcleo.

Solución:

Actualizar Joomla! a la versión 3.9.20.

Detalle:

- La falta de un control de *tokens* en el punto final de *ajax_install com_installer* provoca una vulnerabilidad de CSRF. Se ha asignado el identificador CVE-2020-15695 para esta vulnerabilidad.
- La falta de validación en el objeto de la tabla de grupos de usuarios podría resultar en una configuración de sitio caído. Se ha asignado el identificador CVE-2020-15699 para esta vulnerabilidad.
- La falta de un control de *tokens* en la sección de solicitud de eliminación de *com_privacy* causaría una vulnerabilidad de CSRF. Se ha asignado el identificador CVE-2020-15695 para esta vulnerabilidad.
- Los campos internos de sólo lectura, en la clase de la tabla de usuarios, podrían ser modificados por los usuarios. Se ha asignado el identificador CVE-2020-15697 para esta vulnerabilidad.
- La falta de filtrado de entrada y escape permitiría ataques XSS en *mod_random_image*. Se ha asignado el identificador CVE-2020-15696 para esta vulnerabilidad.
- Un filtrado inadecuado en la pantalla de información del sistema podría exponer credenciales de *redis* o *proxy*. Se ha asignado el identificador CVE-2020-15698 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades XSS en Jenkins

Fecha de publicación: 16/07/2020

Importancia: Alta

Recursos afectados:

- Jenkins hasta versión 2.244 inclusive.
- Jenkins LTS hasta versión 2.235.1 inclusive.

Descripción:

Jenkins ha informado de múltiples vulnerabilidades de tipo Cross-site-scripting (XSS) almacenados que podrían permitir a un atacante remoto ejecutar código arbitrario.

Solución:

Se recomienda instalar las siguientes versiones para solucionar estas vulnerabilidades:

- Jenkins versión 2.245.
- Jenkins LTS versión 2.235.2.

Detalle:

Las vulnerabilidades encontradas en Jenkins afectan a la página de tendencias de tiempo de compilación, al nombre para mostrar del trabajo ascendente, a los iconos de la insignia 'Keep forever', y en la página de la consola de compilación.

Se han asignado los identificadores CVE-2020-2220, CVE-2020-2221, CVE-2020-2222 y CVE-2020-2223 para estas vulnerabilidades. Así mismo, Jenkins ha informado de otras vulnerabilidades en diferentes complementos.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 16/07/2020

Importancia: Crítica

Recursos afectados:

- Cisco PLM Software, versiones 10.5(2)SU9, 11.5(1)SU6 y anteriores;
- Cisco RV215W Wireless-N VPN Router, versiones anteriores a la 1.3.1.7;
- Cisco RV110W Wireless-N VPN Firewall, todas las versiones;
- Cisco RV130 VPN Router, todas las versiones;
- Cisco RV130W Wireless-N Multifunction VPN Router, todas las versiones;
- Cisco RV215W Wireless-N VPN Router, todas las versiones.

Descripción:

Cisco ha publicado múltiples vulnerabilidades, todas ellas de severidad crítica, que podrían permitir a un atacante remoto, no autenticado, conseguir acceso no autorizado al dispositivo, ejecutar código arbitrario u obtener el control total del sistema.

Solución:

Actualizar a las versiones, disponibles desde el panel de descarga de Software de Cisco:

- Cisco PLM 10.5(2)SU10 o superior;
- Cisco PLM 11.5(1)SU7 o superior;
- RV110W Wireless-N VPN Firewall, versión 1.2.2.8;
- RV215W Wireless-N VPN Router, versión 1.3.1.7;
- RV130 VPN Router, versión 1.0.3.55;
- RV130W Wireless-N Multifunction VPN Router, versión 1.0.3.55;
- RV215W Wireless-N VPN Router, versión 1.3.1.7.

Detalle:

- La validación insuficiente de las aportaciones de los usuarios en la interfaz de gestión de la web podría permitir a un atacante que envíe una solicitud maliciosa a un sistema afectado, obtener privilegios de administrador en el sistema. El atacante necesita un nombre de usuario válido para explotar esta vulnerabilidad. Se ha asignado el identificador CVE-2020-3140 para esta vulnerabilidad.
- La validación inadecuada de los datos de entrada proporcionados por el usuario mediante la interfaz de gestión basada en la web podría permitir a un atacante ejecutar código arbitrario con los privilegios del usuario raíz, mediante el envío de solicitudes especialmente diseñadas a un dispositivo específico. Se ha asignado el identificador CVE-2020-3331 para esta vulnerabilidad.
- La gestión inadecuada de las sesiones en los dispositivos afectados podría permitir a un atacante obtener acceso de administrador en el dispositivo afectado, enviando una solicitud HTTP especialmente diseñada al dispositivo afectado. Se ha asignado el identificador CVE-2020-3144 para esta vulnerabilidad.
- La validación inadecuada de los datos suministrados por el usuario en la interfaz de gestión basada en la web podría permitir a un atacante ejecutar código arbitrario como *root* en el sistema operativo subyacente del dispositivo afectado, mediante el envío de solicitudes HTTP especialmente diseñadas a un dispositivo específico. Se ha asignado el identificador CVE-2020-3323 para esta vulnerabilidad.
- Una cuenta del sistema tiene una contraseña predeterminada y estática. Un atacante podría utilizar esta cuenta predeterminada para conectarse al sistema afectado y obtener el control total del dispositivo. Se ha asignado el identificador CVE-2020-3330 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 21/07/2020

Importancia: Alta

Recursos afectados:

- Versión 3.9;
- Desde la versión 3.8, hasta la 3.8.3;
- desde la versión 3.7, hasta la 3.7.6;
- desde la versión 3.5, hasta la 3.5.12;
- versiones anteriores sin soporte.

Descripción:

Se han publicado múltiples vulnerabilidades que podrían permitir a un atacante la denegación del servicio, escalada de privilegios, ataques XXS reflejado o contaminación de prototipo.

Solución:

Moodle ha publicado diversas actualizaciones en función de la versión afectada:

- 3.9.1;
- 3.8.4;
- 3.7.7;
- 3.5.13.

Detalle:

- No limitar la cantidad de archivos que se pueden cargar en la plataforma podría suponer un riesgo de denegación de servicio. Se ha reservado el identificador CVE-2020-14322 para esta vulnerabilidad.
- Los profesores de un curso podrían asignarse a sí mismos el rol de manager dentro de ese curso. Se ha reservado el identificador CVE-2020-14321 para esta vulnerabilidad.
- El saneamiento inadecuado del filtro en el registro de tareas del administrador podría permitir a un atacante llevar a cabo ataques XSS reflejado. Se ha reservado el identificador CVE-2020-14320 para esta vulnerabilidad.
- La versión de JQuery utilizada por la biblioteca H5P podría permitir a un atacante la contaminación de prototipo. Se ha reservado el identificador CVE-2019-11358 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad en Citrix Workspace app

Fecha de publicación: 23/07/2020

Importancia: Alta

Recursos afectados:

Esta vulnerabilidad afecta a las siguientes versiones compatibles de la aplicación Citrix Workspace para Windows:

- Aplicación Citrix Workspace para Windows 1912 LTSR,
- Aplicación Citrix Workspace para Windows 2002.

Esta vulnerabilidad no afecta a la aplicación Citrix Workspace en ninguna otra plataforma, ni a ninguna versión compatible de Citrix Receiver.

Descripción:

Se ha publicado una vulnerabilidad en el servicio de actualización automática de la aplicación Citrix Workspace para Windows que podría permitir a un atacante la escalada de privilegios o comprometer el sistema.

Solución:

Actualizar a las versiones:

- Citrix Workspace App 2006.1 o posterior;
- Citrix Workspace App 1912 LTSR CU1 y posteriores.

Detalle:

La vulnerabilidad presente en el servicio de actualización automática de la aplicación Citrix Workspace para Windows podría permitir a un usuario local la escalada de privilegios al de un administrador o comprometer de manera remota el sistema que ejecuta la aplicación Citrix Workspace cuando se habilita el uso compartido de archivos de Windows (SMB). Se ha reservado el identificador CVE-2020-8207 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, Vulnerabilidad

Protección insuficiente contra las llamadas a API no autorizadas en IBM Verify Gateway

Fecha de publicación: 24/07/2020

Importancia: Alta

Recursos afectados:

- IBM Verify Gateway (IVG) RADIUS 1.0.0;
- IBM Verify Gateway (IVG) PAM 1.0.0, 1.0.1;
- IBM Verify Gateway (IVG) WinLogin 1.0.0, 1.0.1.

Descripción:

La protección insuficiente contra las llamadas a API no autorizadas en IBM Verify Gateway podría permitir a un atacante obtener un token de acceso y utilizarlo con fines maliciosos.

Solución:

Actualizar a las versiones:

- IBM Security Verify Gateway para AIX PAM (Pluggable Authentication Modules) v1.0.1;
- IBM Security Verify Gateway para Linux PAM (Pluggable Authentication Modules) v1.0.2;
- IBM Security Verify Gateway para RADIUS v1.0.1;
- IBM Security Verify Gateway para Windows Login v1.0.2.

Detalle:

Cuando los componentes del IBM Verify Gateway (IVG) hacen llamadas a la API, no hay suficiente protección. Esto podría permitir a un

atacante obtener otros token de acceso y utilizarlos en otra llamada a la API realizando una suplantación.

Etiquetas: Actualización, IBM, Vulnerabilidad

Limitación incorrecta de la ruta a un directorio restringido en Dell EMC OMSA

Fecha de publicación: 28/07/2020

Importancia: Crítica

Recursos afectados:

Dell EMC OpenManage Server Administrator (OMSA), versiones 9.4 y anteriores.

Descripción:

David Yesland, de Rhino Security Labs, ha notificado a Dell EMC una vulnerabilidad, con severidad crítica, de limitación incorrecta del nombre de la ruta a un directorio restringido (*path traversal*), que afecta al producto OpenManage Server Administrator (OMSA).

Solución:

Actualizar Dell EMC OpenManage Server Administrator (OMSA) a las versiones 9.3.0.2 o 9.4.0.2.

Detalle:

Un atacante remoto, no autenticado, podría explotar esta vulnerabilidad al enviar una solicitud de API a la web, especialmente diseñada, que contenga secuencias de caracteres específicas para obtener acceso al sistema de archivos en la estación de administración comprometida. Se ha reservado el identificador CVE-2020-5377 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 30/07/2020

Importancia: Crítica

Recursos afectados:

- Todos los modos de implementación de todos los dispositivos Cisco DCNM que se instalaron utilizando archivos de tipo *.ova* o *.iso*;
- Cisco DCNM, versiones 11.0(1), 11.1(1), 11.2(1) y11.3(1);
- dispositivos Cisco que estén ejecutando una versión vulnerable de Cisco SD-WAN vManage;
- los siguientes productos de Cisco, si están ejecutando una versión vulnerable de Cisco SD-WAN Solution Software:
  - IOS XE SD-WAN Software,
  - SD-WAN vBond Orchestrator Software,
  - SD-WAN vEdge Cloud Routers,
  - SD-WAN vEdge Routers,
  - SD-WAN vManage Software,
  - SD-WAN vSmart Controller Software.

Descripción:

Se han identificado 3 vulnerabilidades de severidad crítica que afectan a múltiples productos de Cisco.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software de Cisco. Para información más detallada, consulte la sección *Referencias*.

Detalle:

- Una vulnerabilidad en la API REST de Cisco Data Center Network Manager (DCNM) podría permitir que un atacante remoto, no autenticado, omitiese la autenticación y ejecutase acciones arbitrarias con privilegios administrativos en el dispositivo afectado. Se ha reservado el identificador CVE-2020-3382 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz web de administración del software Cisco SD-WAN vManage podría permitir que un atacante remoto, autenticado, omitiese la autorización, permitiéndole acceder a información confidencial, modificar la configuración del sistema o afectar la disponibilidad del sistema afectado. Se ha reservado el identificador CVE-2020-3374 para esta vulnerabilidad.
- Una vulnerabilidad en Cisco SD-WAN Solution Software podría permitir que un atacante remoto, no autenticado, causase un desbordamiento de búfer en un dispositivo afectado. Se ha reservado el identificador CVE-2020-3375 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidades en GRUB2 y UEFI Secure Boot

Fecha de publicación: 30/07/2020

Importancia: Alta

Recursos afectados:

Se encuentran afectados por esta vulnerabilidad aquellos sistemas que hagan uso de GRUB2.

Descripción:

Investigadores de seguridad de la empresa Eclypsium han descubierto una vulnerabilidad de desbordamiento de buffer en GRUB2, denominada *BootHole*, que permitiría a un atacante obtener persistencia en el sistema y controlar el proceso de arranque del mismo antes de cargar el sistema operativo.

Solución:

Se recomienda actualizar el *bootloader* o cargador de arranque GRUB2 a su última versión. Las diferentes distribuciones Linux han publicado ya varios parches para cada una.

Otros fabricantes deberán actualizar sus cargadores de arranque y *Shim* (cargador de arranque de primera etapa que incorpora un certificado CA autofirmado) que hacen uso de la CA para *Secure Boot* utilizada por Microsoft y que mantiene las bases de datos de certificados válidos (db) y los revocados (dbx).

Puede consultar la sección de *Referencias* para obtener más información sobre las actualizaciones de diferentes fabricantes.

Detalle:

La vulnerabilidad descubierta se produce por un desbordamiento de búfer en GRUB2, incluso cuando la opción de *Secure Boot* esta activada. El desbordamiento se produce a través del fichero de texto *grub.cfg*, que contiene la secuencia de comandos que se ejecutan durante el arranque, y que es posible modificar con permisos de administrador en los sistemas afectados.

Un atacante con permisos de administrador en el sistema podría modificar el fichero *grub.cfg* y obtener de esa manera acceso al proceso de arranque del sistema antes de cargar el sistema operativo.

El fallo descubierto permite saltarse las opciones de *Secure Boot* disponibles para la firma de *firmware* en los arranques UEFI y el uso de *Shim* que hacen los diferentes fabricantes, invalidando, por lo tanto, el sistema para CA de confianza que permite *bootloaders* o cargadores de arranque de terceros en sistemas UEFI con *Secure Boot* y que gestiona Microsoft.

Esta vulnerabilidad *BootHole* tiene asignado el identificador CVE-2020-10713.

Adicionalmente, Eclypsium ha encontrado otras vulnerabilidades de menor gravedad en GRUB2 con los identificadores CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706 y CVE- 2020-15707.

Etiquetas: Actualización, HP, Linux, Microsoft, VMware, Vulnerabilidad, Windows