Boletín de enero de 2020

Avisos Técnicos

Múltiples vulnerabilidades en productos Cisco DCNM

Fecha de publicación: 03/01/2020

Importancia: Crítica

Recursos afectados:

Cisco Data Center Network Manager (DCNM), versiones anteriores a la 11.3(1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Descripción:

Se han identificado múltiples vulnerabilidades en productos Cisco, 1 de severidad crítica y 3 de severidad alta, que podrían permitir a un atacante remoto realizar acciones arbitrarias con permisos de administrador, ejecutar comandos SQL, realizar ataques de salto de directorio o inyectar comandos en el sistema operativo.

Solución:

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

Detalle:

Las vulnerabilidades de severidad crítica son:

- La clave de cifrado estática se comparte ente diferentes instalaciones de endopoint REST API y endpoint SOAP API, esto podría permitir a un atacante remoto, no autenticado, eludir la autenticación en un dispositivo afectado, utilizando dicha clave estática para crear un token de sesión válido. Se han reservado los identificadores CVE-2019-15975 y CVE-2019-15976 para estas vulnerabilidades.
- La utilización de credenciales estáticas en la interfaz de gestión basada en web de Cisco DCNM podría permitir a un atacante remoto, no autenticado, utilizar dichas credenciales estáticas para autenticarse en la interfaz web y obtener cierta información confidencial de un dispositivo afectado. Esta información podría utilizarse para realizar otros ataques contra el sistema. Se ha reservado el identificador CVE-2019-15977 para esta vulnerabilidad.

Para el resto de vulnerabilidades, de severidad alta, se han reservado los identificadores: CVE-2019-15984, CVE-2019-15985, CVE-2019-15980, CVE-2019-15981, CVE-2019-15982, CVE-2019-15978 y CVE-2019-15979.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de inyección SQL en phpMyAdmin

Fecha de publicación: 08/01/2020

Importancia: Alta

Recursos afectados:

- phpMyAdmin, rama de versiones 4.x anteriores a la 4.9.4,
- phpMyAdmin versión 5.0.0.

Descripción:

CSW Research Labs ha detectado una vulnerabilidad de criticidad alta que afecta a varias versiones de phpMyAdmin. Un atacante podría realizar una inyección SQL.

Solución:

- Versiones de la rama 4.x de phpMyAdmin:
  - Para las versiones 4.8 y 4.9, actualizar a la versión 4.9.4 o superior.
  - Para versiones anteriores, aplicar este parche de seguridad.
- Versiones de la rama 5.x de phpMyAdmin, actualizar a la versión 5.0.1 o superior.

Detalle:

La vulnerabilidad ha sido descubierta en la página de cuentas de usuario. Un atacante podría realizar una inyección SQL. Se ha reservado el identificador CVE-2020-5504 para esta vulnerabilidad.

Etiquetas: Actualización, PHP, Vulnerabilidad

Vulnerabilidad de ejecución de código en e2fsprogs

Fecha de publicación: 08/01/2020

Importancia: Alta

Recursos afectados:

E2fsprogs, versiones 1.43.3 - 1.45.4.

Descripción:

La investigadora Lilith, de Cisco Talos, ha descubierto una vulnerabilidad de tipo ejecución de código en e2fsprogs, un paquete de utilidades para el mantenimiento de sistemas de ficheros ext2, ext3 y ext4.

Solución:

Actualizar e2fsprogs a la versión 1.45.5.

Detalle:

Una vulnerabilidad de escritura fuera de los límites, al comprobar un sistema de archivos dañado de forma maliciosa, podría permitir a un atacante la ejecución arbitraria de código. Esto probablemente no es explotable en plataformas de 64 bits, pero puede serlo en binarios de 32 bits dependiendo de cómo el compilador disponga las variables de pila. Se ha reservado el identificador CVE-2019-5188 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 09/01/2020

Importancia: Alta

Recursos afectados:

- Cisco IOS y Cisco IOS XE, versiones anteriores a 16.1.1 con la funcionalidad *HTTP Server* habilitada.
- Cisco Webex Video Mesh, versiones anteriores a 2019.09.19.1956m.

Descripción:

Se han identificado dos vulnerabilidades en productos Cisco, ambas de severidad alta, que podrían permitir a un atacante remoto realizar CSRF (*Cross-Site Request Forgery*) o inyección de comandos en el sistema afectado.

Solución:

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

Detalle:

- Una vulnerabilidad, de tipo CSRF, detectada en la interfaz de usuario web de los programas Cisco IOS y Cisco IOS XE, en el sistema afectado podría permitir la explotación exitosa de esta vulnerabilidad, autorizando a un atacante remoto, no autenticado, a realizar acciones arbitrarias con el nivel de privilegios del usuario objetivo. Se ha reservado el identificador CVE-2019-16009 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz de gestión basada en la web de Cisco Webex Video Mesh podría permitir que un atacante, remoto y autenticado ejecutar comandos arbitrarios en el sistema operativo Linux subyacente con privilegios de *root* en el nodo objetivo. Se ha reservado el identificador CVE-2019-16005 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos Juniper

Fecha de publicación: 09/01/2020

Importancia: Alta

Recursos afectados:

- Junos OS:

    - 15.1 versiones anteriores a 15.1R7-S6;
    - 15.1X49 versiones anteriores a 15.1X49-D200;
    - 15.1X53 versiones anteriores a 15.1X53-D592;
    - 16.1 versiones anteriores a 16.1R7-S6;
    - 16.2 versiones anteriores a 16.2R2-S11;
    - 17.1 versiones anteriores a 17.1R2-S11, 17.1R3-S1;
    - 17.2 versiones anteriores a 17.2R2-S8, 17.2R3-S3;
    - 17.3 versiones anteriores a 17.3R3-S6;
    - 17.4 versiones anteriores a 17.4R2-S7, 17.4R3;
    - 18.1 versiones anteriores a 18.1R3-S8;
    - 18.2 versiones anteriores a 18.2R3-S2;
    - 18.2X75 versiones anteriores a 18.2X75-D60;
    - 18.3 versiones anteriores a 18.3R1-S6, 18.3R2-S2, 18.3R3;
    - 18.4 versiones anteriores a 18.4R1-S5, 18.4R2-S3, 18.4R3;
    - 19.1 versiones anteriores a 19.1R1-S3, 19.1R2;
    - 19.2 versiones anteriores a 19.2R1-S3, 19.2R2.
- Junos OS Evolved, versiones anteriores a 19.3R1;
- Juniper Networks Junos OS:
    - 16.1 versiones anteriores a 16.1R7-S6;
    - 16.1 versión 16.1X70-D10 y posteriores;
    - 16.2 versiones anteriores a 16.2R2-S11;
    - 17.1 versiones anteriores a 17.1R2-S11, 17.1R3-S1;
    - 17.2 versiones anteriores a 17.2R1-S9, 17.2R2-S8, 17.2R3-S3;
    - 17.3 versiones anteriores a 17.3R3-S6;
    - 17.4 versiones anteriores a 17.4R2-S9, 17.4R3;
    - 18.1 versiones anteriores a 18.1R3-S7;
    - 18.2 versiones anteriores a 18.2R3-S2;
    - 18.2X75 versiones anteriores a 18.2X75-D50, 18.2X75-D410;
    - 18.3 versiones anteriores a 18.3R1-S6, 18.3R2-S2, 18.3R3;
    - 18.4 versiones anteriores a 18.4R2-S2, 18.4R3;
    - 19.1 versiones anteriores a 19.1R1-S3, 19.1R2;
    - 19.2 versiones anteriores a 19.2R1-S2, 19.2R2.
    - 12.3 versiones anteriores a 12.3R12-S15;
    - 12.3X48 versiones anteriores a 12.3X48-D86, 12.3X48-D90 en SRX Series;
    - 14.1X53 versiones anteriores a 14.1X53-D51 en EX y QFX Series;
    - 15.1F6 versiones anteriores a 15.1F6-S13;
    - 15.1 versiones anteriores a 15.1R7-S5;
    - 15.1X49 versiones anteriores a 15.1X49-D181, 15.1X49-D190 en SRX Series;
    - 15.1X53 versiones anteriores a 15.1X53-D238 en QFX5200/QFX5110 Series;
    - 15.1X53 versiones anteriores a 15.1X53-D592 en EX2300/EX3400 Series;
    - 16.1 versiones anteriores a 16.1R4-S13, 16.1R7-S5;
    - 16.2 versiones anteriores a 16.2R2-S10;
    - 17.1 versiones anteriores a 17.1R2-S11, 17.1R3-S1;
    - 17.2 versiones anteriores a 17.2R1-S9, 17.2R3-S2;
    - 17.3 versiones anteriores a 17.3R2-S5, 17.3R3-S5;
    - 17.4 versiones anteriores a 17.4R2-S6, 17.4R3;
    - 18.1 versiones anteriores a 18.1R3-S7;
    - 18.2 versiones anteriores a 18.2R2-S5, 18.2R3;
    - 18.3 versiones anteriores a 18.3R1-S6, 18.3R2-S1, 18.3R3;
    - 18.4 versiones anteriores a 18.4R1-S5, 18.4R2;
    - 19.1 versiones anteriores a 19.1R1-S2, 19.1R2.
- MX Series con Juniper Networks Junos OS:
    - 17.2 versiones 17.2R2-S6, 17.2R3 y posteriores;
    - 17.3 versiones anteriores a 17.3R2-S5, 17.3R3-S5;
    - 17.4 versiones anteriores a 17.4R2-S7,17.4R3;
    - 18.1 versiones anteriores a 18.1R3-S6;
    - 18.2 versiones anteriores a 18.2R3-S2;
    - 18.2X75 versiones anteriores a 18.2X75-D51, 18.2X75-D60;
    - 18.3 versiones anteriores a 18.3R3;
    - 18.4 versiones anteriores a 18.4R2;
    - 19.1 versiones anteriores a 19.1R1-S3, 19.1R2;
    - 19.2 versiones anteriores a 19.2R1-S2, 19.2R2.

Descripción:

Se han publicado múltiples vulnerabilidades en productos Juniper que podrían permitir a un atacante ejecutar comandos como *root*, provocar la denegación del servicio, secuestrar la sesión J-Web para llevar a cabo acciones de administración o provocar el cierre inesperado y el reinicio del dispositivo.

Solución:

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

Detalle:

- El modo JDHCPD de Juniper Network podría permitir a un atacante enviar paquetes especialmente diseñados para ejecutar comandos arbitrarios como *root* en el dispositivo de destino o hacerse cargo de la ejecución de código del proceso JDHDCP. Se han reservado los identificadores CVE-2020-1602, CVE-2020-1605 y CVE-2020-1609 para esta vulnerabilidad.
- El manejo incorrecto de los paquetes específicos de IPv6, enviados por los clientes, puede causar que el tráfico de IPv6 de los dispositivos del cliente se pierda y provocar una pérdida de memoria dentro del dispositivo que conduzca a un bloqueo del *kernel* (*vmcore*) creando una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2020-1603 para esta vulnerabilidad.
- Una protección insuficiente contra ataques de *Cross-Site Scripting* (XSS) en J-Web puede permitir a un atacante, remoto, inyectar secuencias de comandos web o HTML, secuestrar la sesión de J-Web del usuario objetivo o realizar acciones administrativas en el dispositivo Junos como otro usuario. Se ha reservado el identificador CVE-2020-1607 para esta vulnerabilidad.
- La recepción de un paquete MPLS o IPv6 específico en la interfaz del *core* de un dispositivo de la serie MX, configurado para el servicio Broadband Edge (BBE), puede provocar el cierre inesperado de *vmcore*, haciendo que el dispositivo se reinicie. Se ha reservado el identificador CVE-2020-1608 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de enero de 2020

Fecha de publicación: 15/01/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- ASP.NET Core;
- .NET Core;
- .NET Framework;
- OneDrive para Android;
- Microsoft Dynamics;

Descripción:

La publicación de actualizaciones de seguridad de Microsoft correspondiente al mes de enero consta de 50 vulnerabilidades, 8 clasificadas como críticas y 42 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:

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

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Actualización de seguridad de SAP de enero de 2020

Fecha de publicación: 15/01/2020

Importancia: Media

Recursos afectados:

- SAP Process Integration - Rest Adapter (SAP_XIAF), versiones - 7.31, 7.40, 7.50;
- SAP NetWeaver Internet Communication Manager, versiones:
  - KRNL32NUC y KRNL32UC 7.21, 7.21EXT, 7.22 y 7.22EXT;
  - KRNL64NUC y KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT y 7.49;
  - KERNEL 7.21, 7.22, 7.49 y 7.53;
- RTCISM, versión - 100;
- SAP Disclosure Management, versión - 10.1;
- Automated Note Search Tool (SAP Basis), versiones - 7.0, 7.01,7.02, 7.31, 7.4, 7.5, 7.51, 7.52, 7.53 y 7.54;
- SAP UI, versiones - 7.5, 7.51, 7.52, 7.53 y 7.54;
- SAP UI 700, versión - 2.0;
- SAP Leasing, versiones:
  - (SAP_Appl) 6.18;
  - (EA_Appl) 6.0, 6.02, 6.03, 6.04, 6.05, 6.06, 6.16 y 6.17;

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 una actualización, siendo la actualización y 4 de las notas de severidad media y otra de las notas de severidad baja.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de falta de comprobación de autorización;
- 1 vulnerabilidad de suplantación de contenido;
- 1 vulnerabilidad de DoS (*Denial of Service*);
- 1 vulnerabilidad de XSS (*Cross-Site Scripting*);
- 1 vulnerabilidad de otro tipo.

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-6305, CVE-2020-6304, CVE-2020-6303, CVE-2020-6307, CVE-2019-0388 y CVE-2020-6306.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad en VMware Tools

Fecha de publicación: 15/01/2020

Importancia: Alta

Recursos afectados:

- VMware Tools, versión 10.x.y para Windows.

Descripción:

Se ha publicado una vulnerabilidad de criticidad alta. Un atacante local podría realizar una escalada de privilegios en el sistema.

Solución:

- Se recomienda actualizar a VMware Tools a la versión 11.0.0 y posteriores.
- Si no es posible actualizar, se puede prevenir su explotación siguiendo estas indicaciones de VMware.

Detalle:

La operación de reparación de VMware Tools para Windows tiene una condición de carrera. Un atacante, en la máquina virtual invitada, podría escalar privilegios en una máquina virtual de Windows. Se ha reservado el identificador CVE-2020-3941 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad

Actualizaciones críticas en Oracle (enero 2020)

Fecha de publicación: 15/01/2020

Importancia: Crítica

Recursos afectados:

- Enterprise Manager Base Platform, versiones 12.1.0.5, 13.2.0.0, 13.3.0.0;
- Enterprise Manager para Fusion Middleware, versiones 13.2.0.0, 13.3.0.0;
- Enterprise Manager para Oracle Database, versiones 12.1.0.5, 13.2.0.0, 13.3.0.0;
- Enterprise Manager Ops Center, versiones 12.3.3, 12.4.0;
- Hyperion Financial Close Management, versión 11.1.2.4;
- Hyperion Planning, versión 11.1.2.4;
- Identity Manager, versiones 11.1.2.3.0, 12.2.1.3.0;
- Instantis EnterpriseTrack, versiones 17.1, 17.2, 17.3;
- JD Edwards EnterpriseOne Orchestrator, versión 9.2;
- JD Edwards EnterpriseOne Tools, versión 9.2;
- MySQL Client, versiones 5.6.46 y anteriores, 5.7.28 y anteriores, 8.0.18 y anteriores;
- MySQL Cluster, versiones 7.3.27 y anteriores, 7.4.25 y anteriores, 7.5.15 y anteriores, 7.6.12 y anteriores;
- MySQL Connectors, versiones 5.3.13 y anteriores, 8.0.18 y anteriores;
- MySQL Enterprise Backup, versiones 3.12.4 y anteriores, 4.1.3 y anteriores;
- MySQL Server, versiones 5.6.46 y anteriores, 5.7.28 y anteriores, 8.0.18 y anteriores;
- MySQL Workbench, versiones 8.0.18 y anteriores;
- Oracle Agile Engineering Data Management, versiones 6.2.0, 6.2.1;
- Oracle Agile PLM, versiones 9.3.3, 9.3.4, 9.3.5, 9.3.6;
- Oracle Agile PLM Framework, versión 9.3.3;
- Oracle Agile PLM MCAD Connector, versiones 3.4, 3.5, 3.6;
- Oracle Application Testing Suite, versiones 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1;
- Oracle AutoVue, versión 12.0.2;
- Oracle Banking Corporate Lending, versiones 12.3.0-12.4.0, 14.0.0-14.3.0;
- Oracle Banking Payments, versiones 14.1.0-14.3.0;
- Oracle Big Data Discovery, versión 1.6;
- Oracle Business Intelligence Enterprise Edition, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Clinical, versión 5.2;
- Oracle Coherence, versiones 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Communications Design Studio, versiones 7.3.4.3.0, 7.3.5.5.0, 7.4.0.4.0, 7.4.1.1.0;
- Oracle Communications Diameter Signaling Router (DSR), versiones 8.0, 8.1, 8.2, 8.3, 8.4;
- Oracle Communications Instant Messaging Server, versión 10.0.1.3.0;
- Oracle Communications Interactive Session Recorder, versiones 6.0, 6.1, 6.2, 6.3;
- Oracle Communications IP Service Activator, versiones 7.3.4, 7.4.0;
- Oracle Communications Session Border Controller, versiones 7.4, 8.0, 8.1, 8.2, 8.3;
- Oracle Communications Session Router, versiones 7.4, 8.0, 8.1, 8.2, 8.3;
- Oracle Communications Subscriber-Aware Load Balancer, versiones 7.3, 8.1, 8.3;
- Oracle Communications Unified Inventory Management, versiones 7.3, 7.4;
- Oracle Communications Unified Session Manager, versiones 7.3.5, 8.2.5;
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.1.0.11, 12.2.0.1, 18c, 19c, 29, 212.2.0.1;
- Oracle Demantra Demand Management, versiones 12.2.4, 12.2.4.1, 12.2.5, 12.2.5.1;
- Oracle E-Business Suite, versiones 12.1.1-12.1.3, 12.2.3-12.2.9;
- Oracle Endeca Information Discovery Integrator, versión 3.2.0;
- Oracle Endeca Information Discovery Studio, versión 3.2.0;
- Oracle Enterprise Communications Broker, versiones PCz3.0, PCz3.1, PCz3.2;
- Oracle Enterprise Repository, versión 12.1.3.0.0;
- Oracle Enterprise Session Border Controller, versiones 7.5, 8.0, 8.1, 8.2, 8.3;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 7.3.3-7.3.5, 8.0.0-8.0.8;
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.2-8.0.7;
- Oracle Financial Services Revenue Management y Billing, versiones 2.7.0.0, 2.7.0.1, 2.8.0.0;
- Oracle FLEXCUBE Investor Servicing, versiones 12.1.0-12.4.0, 14.0.0-14.1.0;
- Oracle FLEXCUBE Universal Banking, versiones 12.0.1-12.4.0, 14.0.0-14.3.0;
- Oracle GraalVM Enterprise Edition, versión 19.3.0.2;

- Oracle Health Sciences Data Management Workbench, versiones 2.4, 2.5;
- Oracle Healthcare Master Person Index, versión 3.0;
- Oracle Hospitality Cruise Materials Management, versión 7.30.567;
- Oracle Hospitality Guest Access, versión 4.2;
- Oracle Hospitality OPERA 5, versiones 5.5, 5.6;
- Oracle Hospitality Suites Management, versiones 3.7, 3.8;
- Oracle HTTP Server, versiones 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0;
- Oracle iLearning, versión 6.1;
- Oracle Java SE, versiones 7u241, 8u231, 8u241, 11.0.5, 13.0.1;
- Oracle Java SE Embedded, versión 8u231;
- Oracle Outside In Technology, versión 8.5.4;
- Oracle Real-Time Scheduler, versiones 2.3.0.1-2.3.0.3;
- Oracle Reports Developer, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Retail Assortment Planning, versiones 15.0.3, 16.0.3;
- Oracle Retail Clearance Optimization Engine, versiones 13.4, 14.0, 14.0.3, 14.0.5;
- Oracle Retail Customer Management y Segmentation Foundation, versiones 16.0, 17.0, 18.0;
- Oracle Retail Markdown Optimization, versiones 13.4, 13.4.4;
- Oracle Retail Order Broker, versiones 5.2, 15.0, 16.0, 18.0;
- Oracle Retail Predictive Application Server, versiones 15.0.3, 16.0.3;
- Oracle Retail Sales Audit, versión 15.0.3.16.0.2;
- Oracle Secure Global Desktop, versiones 5.4, 5.5;
- Oracle Security Service, versiones 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0;
- Oracle Solaris, versiones 10, 11;
- Oracle Tuxedo, versiones 12.1.1.0.0, 12.1.3.0.0;
- Oracle Utilities Framework, versiones 4.2.0.2-4.2.0.3, 4.3.0.1-4.3.0.4;
- Oracle Utilities Mobile Workforce Management, versiones 2.3.0.1-2.3.0.3;
- Oracle Utilities Work y Asset Management (v1), versión 1.9.1.2;
- Oracle VM Server para SPARC, versión 3.6;
- Oracle VM VirtualBox, versiones anteriores a 5.2.36, anteriores a 6.0.16, anteriores a 6.1.2;
- Oracle WebCenter Sites, versión 12.2.1.3.0;
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0;
- PeopleSoft Enterprise CC Common Application Objects, versiones 9.1, 9.2;
- PeopleSoft Enterprise HCM Human Resources, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57, 8.58;
- PeopleSoft PeopleTools, versiones 8.56, 8.57;
- Primavera Gateway, versiones 15.2.18, 16.2.11, 17.12.6, 18.8.8.1;
- Primavera P6 Enterprise Project Portfolio Management, versiones 15.1.0.0-15.2.18.7, 16.1.0.0-16.2.19.0, 17.1.0.0-17.12.16.0, 18.1.0.0-18.8.16.0, 19.12.0.0, 20.1.0.0;
- Primavera Unifier, versiones 16.1, 16.2, 17.7-17.12, 18.8, 19.12;
- Siebel Applications, versiones 19.10 y anteriores;
- Sun ZFS Storage Appliance Kit, versión 8.8.6;
- Tape Library ACSLS, versiones 8.5, 8.5.1;

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 255 vulnerabilidades (con 334 parches), algunas de las cuales son críticas. El detalle de las vulnerabilidades resueltas se puede consultar en el enlace de Oracle de la sección de *Referencias*.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Vulnerabilidad en VTune Amplifier para Windows de Intel

Fecha de publicación: 15/01/2020

Importancia: Alta

Recursos afectados:

Intel VTune Amplifier para Windows, versiones anteriores a la actualización 8.

Descripción:

Intel ha detectado una vulnerabilidad de criticidad alta. Un atacante local podría realizar una escalada de privilegios en el sistema.

Solución:

Aplicar la actualización 8 o posterior de Intel VTune Amplifier para Windows.

Detalle:

Un control de acceso inapropiado en el driver para Intel VTune Amplifier para Windows podría permitir a un atacante local realizar una escalada de privilegios en el sistema. Se ha reservado el identificador CVE-2019-14613 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en Superdome Flex Server de HPE

Fecha de publicación: 16/01/2020

Importancia: Alta

Recursos afectados:

HPE Superdome Flex Server, versión 3.20.186 y anteriores.

Descripción:

HPE ha detectado una vulnerabilidad de criticidad alta que afecta a su servidor Flex Superdome. Un atacante remoto, con privilegios de administrador, podría revelar información.

Solución:

Actualizar el *firmware* del dispositivo a la versión 3.20.206 o posterior.

Detalle:

La vulnerabilidad se debe a una comprobación de entrada inapropiada de los comandos de administrador. Un atacante remoto, con privilegios de administrador, podría evadir las restricciones de seguridad y revelar información. Se ha reservado el identificador CVE-2019-11998 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad de XSS almacenado en Moodle

Fecha de publicación: 20/01/2020

Importancia: Alta

Recursos afectados:

Moodle, versión 3.8.

Descripción:

El investigador, Cid da Costa, ha detectado una vulnerabilidad de criticidad alta en Moodle. Un atacante remoto podría ejecutar código arbitrario en el sistema.

Solución:

- Actualizar Moodle a la versión 3.8.1.
- Como medida preventiva, Moodle recomienda deshabilitar el sistema de mensajería hasta aplicar la actualización.

Detalle:

La vulnerabilidad es debida a una sanitización inadecuada antes de actualizar el resumen de las conversaciones. Un atacante podría realizar un ataque de Cross-site-scripting (XSS) almacenado y ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-1691 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Denegación de servicio en las familias Unity y Unity XT de Dell EMC

Fecha de publicación: 21/01/2020

Importancia: Alta

Recursos afectados:

- Dell EMC Unity y Unity XT Operating Environment (OE) versiones anteriores a la 5.0.2.0.5.009;
- Dell EMC Unity VSA Operating Environment (OE) versiones anteriores a la 5.0.2.0.5.009.

Descripción:

Dell EMC ha detectado una vulnerabilidad de criticidad alta. Un atacante remoto, sin autenticación, podría generar una condición de denegación de servicio (DoS).

Solución:

- Actualizar Dell EMC Unity y Dell EMC Unity XT Operating Environment (OE) a la versión 5.0.2.0.5.009 o posterior;
- Dell EMC Unity VSA Operating Environment (OE) a la versión 5.0.2.0.5.009 o posterior.

Detalle:

La vulnerabilidad reside en la implementación del SSH empleada para el servicio SFTP en el servidor NAS. Un atacante remoto, sin autenticación, podría generar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2020-5319 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Divulgación de clave privada del certificado TLS en routers Netgear

Fecha de publicación: 23/01/2020

Importancia: Alta

Recursos afectados:

Routers de los modelos:

- R8900;
- R9000;
- RAX120;
- XR700.

Descripción:

Netgear ha publicado un aviso, de severidad alta, informando de una vulnerabilidad de divulgación de clave privada del certificado TLS.

Solución:

NETGEAR planea lanzar *hotfixes* de *firmware* para todos los productos afectados tan pronto como sea posible. Hasta entonces, el fabricante recomienda utilizar la App NETGEAR Nightawk o hacer *login* en la interfaz web del router utilizando HTTP (http://routerlogin.com) en lugar de HTTPS.

Detalle:

Los productos afectados utilizan certificados firmados por una Autoridad de Certificación (CA) para proporcionar acceso seguro con HTTPS a su interfaz web. Al intentar acceder a la interfaz web del router mediante HTTPS es posible que aparezca un mensaje de error o una advertencia del certificado de seguridad.

Etiquetas: SSL/TLS, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 23/01/2020

Importancia: Crítica

Recursos afectados:

- Cisco FMC Software, si está configurado para autenticar a los usuarios de la interfaz web de gestión a través de un servidor LDAP externo;
- Cisco TelePresence:
  - Integrator C Series;
  - MX Series;
  - SX Series;
  - System EX Series.
- Cisco Webex:
  - Board;
  - DX Series;
  - Room Series.
- Cisco IOS XE SD-WAN Software, versiones 16.11 y anteriores;
- Cisco SD-WAN Solution vManage Software, versión 18.4.1;
- Cisco Smart Software Manager On-Prem. versiones anteriores a 7-201910;
- Cisco IOS XR Software, versiones posteriores a 6.6.1, o anteriores a 6.6.3, 7.0.2, 7.1.1, o 7.2.1.

Descripción:

Se han identificado 12 vulnerabilidades en productos Cisco, una de severidad crítica y el resto de severidad alta, que podrían permitir omisión de autenticación en LDAP, acceso a rutas no controlado, credenciales por defecto, escalada de privilegios o denegación de servicio.

Solución:

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

Detalle:

- La vulnerabilidad de severidad crítica podría permitir a un atacante remoto, no autenticado, omitir la autenticación del protocolo LDAP y realizar acciones arbitrarias con privilegios de administrador en el dispositivo afectado. Se ha reservado el identificador CVE-2019-16028 para esta vulnerabilidad.
- El resto de vulnerabilidades, de severidad alta, podrían permitir realizar los siguientes tipos de ataque:
  - acceso a rutas no controlado;
  - uso de credenciales por defecto;
  - escalada local de privilegios;
  - denegación de servicio.

Para las vulnerabilidades de severidad alta, se han reservado los siguientes identificadores: CVE-2020-3143, CVE-2019-1950, CVE-2020-3115, CVE-2019-16029, CVE-2019-16018, CVE-2019-16019, CVE-2019-16020, CVE-2019-16021, CVE-2019-16022, CVE-2019-16023 y CVE-2019-16027.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Omisión de restricciones de seguridad en MQ Appliance de IBM

Fecha de publicación: 24/01/2020

Importancia: Alta

Recursos afectados:

- IBM MQ Appliance, versión 8.0;
- IBM MQ Appliance, versión 9.1 LTS;
- IBM MQ Appliance, versión 9.1 CD.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta que afecta a sus productos MQ Appliance. Un atacante local podría omitir las restricciones de seguridad.

Solución:

- IBM MQ Appliance versión 8, actualizar a la versión 8.0.0.14 o posterior.
- IBM MQ Appliance versión 9.1 LTS, actualizar a la versión 9.1.0.4 o posterior.
- IBM MQ Appliance versión 9.1 CD, actualizar a la versión 9.1.4 o posterior.

Detalle:

La vulnerabilidad se debe a una validación incorrecta de las variables de entorno. Un atacante local podría omitir las restricciones de seguridad. Se ha reservado el CVE-2019-4620 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de acceso a reuniones sin autenticación en Cisco Webex

Fecha de publicación: 27/01/2020

Importancia: Alta

Recursos afectados:

- Cisco Webex Meetings Suite, versiones anteriores a 39.11.5;
- Cisco Webex Meetings Online, versiones anteriores a 40.1.3.

Descripción:

Se ha identificado una vulnerabilidad de severidad alta en productos Cisco, que podría permitir que un atacante remoto no autentificado ingresase en una reunión de videoconferencia protegida con contraseña.

Solución:

Las actualizaciones que corrigen la vulnerabilidad indicada pueden descargarse desde el panel de descarga de Software de Cisco.

Detalle:

- Una vulnerabilidad en los productos Cisco Webex Meetings Suite y Cisco Webex Meetings Online podría permitir a un asistente remoto, no autenticado, unirse a una reunión protegida por contraseña sin proporcionar la contraseña de la reunión. El intento de conexión debe iniciarse desde una aplicación móvil de Webex para iOS o Android. Se ha asignado el identificador CVE-2020-3142 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos IBM

Fecha de publicación: 27/01/2020

Importancia: Crítica

Recursos afectados:

- IBM Security Secret Server, todas las versiones;
- IBM WIoTP MessageGateway, versión 5.0.0.1;
- IBM IoT MessageSight, versión 5.0.0.0;
- IBM IoT MessageSight, versión 2.0.

Descripción:

IBM ha detectado dos vulnerabilidades, una de severidad alta y otra crítica, que afectan a varios productos. Un atacante remoto podría ejecutar código arbitrario en el sistema, generar una condición de denegación de servicio (DoS), u obtener información sensible.

Solución:

- IBM Security Secret Server, actualizar a la versión 10.7 o posterior;
- IBM WIoTP MessageGateway, actualizar a la versión 5.0.0.2;
- IBM MessageSight, actualizar a la versión 5.0.0.0;

- IBM MessageSight, actualizar a la versión 2.0.0.2.

Detalle:

- La vulnerabilidad de severidad crítica afecta a los dispositivos Watson IoT MessageGateway Server. Estos dispositivos son vulnerables a un desbordamiento de bufer cuando gestionan peticiones HTTP fallidas con contenido específicamente formado en sus cabeceras. Un atacante remoto podría ejecutar código arbitrario o generar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2020-4207 para esta vulnerabilidad.
- La vulnerabilidad de criticidad alta afecta a Security Secret Server. Los dispositivos son vulnerables a un ataque de redireccionamiento abierto, pudiendo generar sitios web específicamente creados para engañar a la víctima. Un atacante remoto podría obtener información sensible. Se ha reservado el identificador CVE-2019-4631 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de inyección XXE en IBM Security Access Manager

Fecha de publicación: 28/01/2020

Importancia: Alta

Recursos afectados:

IBM Security Access Manager (ISAM), versión 9.0.

Descripción:

Varios investigadores de IBM X-Force Ethical Hacking Team han descubierto una vulnerabilidad con severidad alta, de tipo *XML External Entity* (XXE), en IBM Security Access Manager.

Solución:

Actualizar IBM Security Access Manager a la versión 9.0.7.1.

Detalle:

IBM Security Access Manager (ISAM) es vulnerable a un ataque de tipo *XML External Entity* (XXE) cuando procesa datos XML. Un atacante remoto podría explotar esta vulnerabilidad para exponer información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2019-4707 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de XSS en TIBCO Patterns - Search

Fecha de publicación: 29/01/2020

Importancia: Alta

Recursos afectados:

TIBCO Patterns - Search, versión 5.4.0 y anteriores.

Descripción:

TIBCO ha detectado una vulnerabilidad de criticidad alta que afecta a su producto TIBCO Patterns - Search. Un atacante remoto podría obtener todos los privilegios del sistema.

Solución:

Actualizar TIBCO Patterns - Search a la versión 5.5.0 o superior.

Detalle:

La interfaz de usuario TIBCO Patterns - Search es vulnerable a un ataque de tipo Cross-Site Scripting (XSS). Un atacante remoto podría obtener todos los privilegios del sistema. Se ha asignado el identificador CVE-2019-17388 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.15

Fecha de publicación: 29/01/2020

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones desde la 3.0.0, hasta la 3.9.14.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 3 vulnerabilidades de criticidad baja en su núcleo, de los tipos CSRF y XSS.

Solución:

Actualizar a la versión 3.9.15.

Detalle:

- La falta de controles simbólicos en las acciones de los lotes de varios componentes causa vulnerabilidades de tipo CSRF (*Cross-Site Request Forgery*). Se ha asignado el identificador CVE-2020-8419 para esta vulnerabilidad.
- La falta de comprobación en el *token* de ataques de tipo CSRF dentro del compilador *LESS* de *com_templates* puede causar un ataque de esta naturaleza. Se ha asignado el identificador CVE-2020-8420 para esta vulnerabilidad.
- El escape inadecuado de los nombres de usuario permite realizar ataques de tipo XSS (*Cross-Site Scripting*) en *com_actionlogs*. Se ha asignado el identificador CVE-2020-8421 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de autorización inapropiada en Dell EMC Isilon OneFS

Fecha de publicación: 30/01/2020

Importancia: Alta

Recursos afectados:

Dell EMC Isilon OneFS, versiones:

- 8.1.2;
- 8.1.0.4;
- 8.1.0.3;
- 8.0.0.7.

Descripción:

Dell EMC ha detectado una vulnerabilidad, de criticidad alta, que permitiría a un atacante remoto comprometer el equipo afectado mediante el acceso a archivos restringidos.

Solución:

- Para las versiones 8.2.0 o posteriores, la actualización de seguridad está contenida en la propia versión.
- Para las versiones 8.1.0.4 y 8.1.2, la corrección se incluye en el *Rollup Patch* de septiembre de 2019, así como en todos los *Rollup Patches* futuros. Se puede obtener más información consultando el documento Current Isilon OneFS Patches.
- Para la versión 8.0.0.7, se recomienda actualizar a una versión más reciente de OneFS.

Detalle:

Los componentes de servicio de archivos HTTP y WebDAV, que no sean RAN, contienen una vulnerabilidad en la que cuando cualquiera de ellos está activado, además de la autenticación básica para uno o ambos componentes, los archivos son accesibles sin autenticación, lo que permitiría a un atacante remoto acceder a archivos restringidos. Se ha reservado el identificador CVE-2020-5318 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 30/01/2020

Importancia: Alta

Recursos afectados:

- Jenkins LTS, versión 2.204.1 y anteriores;
- Jenkins weekly, versión 2.218 y anteriores.

Descripción:

Jenkins ha detectado 7 vulnerabilidades, una de criticidad baja, cinco medias y una alta, que afectan a su *core*. Un atacante remoto, sin autenticación, podría comprometer el cifrado de las comunicaciones, generar una condición de denegación de servicio en el sistema u obtener información del mismo.

Solución:

- Jenkins LTS, actualizar a la versión 2.204.2;
- Jenkins weekly, actualizar a la versión 2.219.

Detalle:

- La vulnerabilidad de criticidad alta se debe a una incorrecta reutilización de los parámetros de cifrado en el protocolo. Un atacante remoto, sin autenticar, podría comprometer el cifrado de las comunicaciones y conectarse desde los agentes Jenkins comprometidos al Jenkins maestro. Se ha asignado el identificador CVE-2020-2099 para esta vulnerabilidad.
- A las vulnerabilidades de criticidad media se las han reservado los identificadores: CVE-2020-2100, CVE-2020-2101, CVE-2020-2102, CVE-2020-2103, CVE-2020-2104.
- A la vulnerabilidad de criticidad baja se le ha asignado el identificador CVE-2020-2105.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Small Business Switches de Cisco

Fecha de publicación: 30/01/2020

Importancia: Alta

Recursos afectados:

- Los siguientes productos Cisco que utilicen un *firmware* anterior a la versión 2.5.0.92:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches;
  - 550X Series Stackable Managed Switches.
- Los siguientes productos Cisco que utilicen un *firmware* anterior a la versión 1.4.11.4:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.
- Los siguientes productos Cisco que utilicen un *firmware* anterior a la versión 1.3.7.18:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.

Descripción:

El investigador, Ken Pyle, de DFDR Consulting LLC, ha notificado a Cisco la existencia de dos vulnerabilidades de criticidad alta en sus Small Business Switches. Un atacante remoto, sin autenticación, podría generar una condición de denegación de servicio (DoS) o acceder a información sensible de los dispositivos.

Solución:

- Actualizar los siguientes productos de Cisco a la versión de *firmware* 2.5.0.92: (CVE-2019-15993)
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches;
  - 550X Series Stackable Managed Switches.
- Actualizar los siguientes productos de Cisco a la versión de *firmware* 1.4.11.4: (CVE-2019-15993)
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.
- Actualizar los siguientes productos de Cisco a la versión de *firmware* 1.3.7.18: (CVE-2020-3147)
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.

Detalle:

- Una vulnerabilidad en la interfaz de usuario web podría permitir a un atacante remoto, no autenticado, enviar una petición HTTP maliciosa y obtener información sensible del dispositivo. Se ha reservado el identificador CVE-2019-15993 para esta vulnerabilidad.
- Una falta de validación en las peticiones enviadas a la interfaz web podrían permitir a un atacante remoto enviar peticiones maliciosas y generar una condición de denegación de servicio (DoS) en el dispositivo. Se ha asignado el identificador CVE-2020-3147 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de denegación de servicio en IBM WebSphere Application Server

Fecha de publicación: 31/01/2020

Importancia: Alta

Recursos afectados:

- WebSphere Application Server, versiones:
  - 9.0;
  - 8.5;
  - 8.0;
  - 7.0.
- WebSphere Application Server Liberty: entrega continua.

Descripción:

Se ha descubierto una vulnerabilidad, de severidad alta, de tipo denegación de servicio en el producto WebSphere Application Server de IBM.

Solución:

- Para WebSphere Application Server y WebSphere Application Server Hypervisor Edition, en las versiones:
  - desde 9.0.0.0 hasta 9.0.5.2:
    - actualizar a los niveles mínimos del *fix pack* según lo requerido por el *interim fix* PH19528 (parche provisional) y luego aplicarlo;
    - aplicar el *fix pack* 9.0.5.3 o posterior (previsión de disponibilidad: primer trimestre 2020);
  - desde 8.5.0.0 hasta 8.5.5.17:
    - actualizar a los niveles mínimos del paquete de *fix pack* según lo requerido por el *interim fix* PH19528 y luego aplicarlo;

        - aplicar el *fix pack* 8.5.5.18 o posterior (previsión de disponibilidad: tercer trimestre 2020);
    - desde 8.0.0.0 hasta 8.0.0.15: actualizar a 8.0.0.15 y luego aplicar el *interim fix* PH19528;
    - desde 7.0.0.0 hasta 7.0.0.45: actualizar a 7.0.0.45 y luego aplicar el *interim fix* PH19528.
- Para WebSphere Application Server Liberty utilizando la funcionalidad *transportSecurity-1.0*:
    - actualizar a los niveles mínimos del *fix pack* según lo requerido por el *interim fix* PH19528 y luego aplicarlo;
    - aplicar el *fix pack* 20.0.0.2 o posterior (previsión de disponibilidad: primer trimestre 2020).

Detalle:

IBM WebSphere Application Server es vulnerable a una denegación de servicio, causada por el envío de una solicitud especialmente diseñada. Un atacante remoto podría explotar esta vulnerabilidad para hacer que el servidor consuma toda la memoria disponible. Se ha reservado el identificador CVE-2019-4720 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Validación insuficiente en el servidor de correo OpenSMTPD de OpenBSD

Fecha de publicación: 31/01/2020

Importancia: Crítica

Recursos afectados:

OpenSMTPD, versiones:

- 6.0.2p1-2;
- 6.0.3p1-5;
- 6.6.1p1-5~bpo10 1.

Descripción:

Investigadores de Qualys Research Labs han descubierto una vulnerabilidad en una función de OpenSMTPD, que puede ser explotada para ejecutar código arbitrario con permisos de *root* en un servidor vulnerable.

Solución:

Actualizar OpenSMTPD a las versiones:

- 6.0.2p1-2 deb9u2;
- 6.0.3p1-5 deb10u3;
- 6.6.2p1-1.

Detalle:

La vulnerabilidad se ha detectado en el modo en que OpenSMTPD valida la dirección del remitente, a través de una función vulnerable, llamada *smtp_mailaddr()*. Esta función puede ser explotada para ejecutar código arbitrario con permisos de *root* en un servidor vulnerable, mediante el envío de un mensaje SMTP especialmente diseñado. Se ha asignado el identificador CVE-2020-7247 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Linux, Privacidad, Vulnerabilidad