Boletín de abril de 2020

Avisos Técnicos

Vulnerabilidad de falta de seguridad del protocolo DTLS en GnuTLS

Fecha de publicación: 01/04/2020

Importancia: Alta

Recursos afectados:

GnuTLS, versión 3.6.3.

Descripción:

Se ha detectado una vulnerabilidad, de severidad alta, en el protocolo DTLS utilizado por GnuTLS.

Solución:

Actualizar GnuTLS a la versión 3.6.13 o posteriores.

Detalle:

Se ha descubierto que GnuTLS 3.6.3 introdujo una regresión en la implementación del protocolo DTLS (*Datagram Transport Layer Security*). Este hecho originó que el cliente DTLS no contribuyera a la negociación DTLS, rompiendo las garantías de seguridad del protocolo DTLS.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad

Desbordamiento de búfer en algunas aplicaciones Aspera de IBM

Fecha de publicación: 01/04/2020

Importancia: Alta

Recursos afectados:

Todas las versiones de los productos:

- Aspera High Speed Transfer Server,
- Aspera High Speed Transfer Endpoint,
- Aspera Proxy,
- Aspera Transfer Cluster Manager,
- Aspera Application on Demand,
- Aspera Faspex on Demand,
- Aspera Server on Demand,
- Aspera Shares on Demand,
- Aspera Streaming,
- Aspera High Speed Transfer Server para Cloudpak para Integration (CP4I).

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta que afecta a algunas de sus aplicaciones Aspera. Un atacante remoto, con conocimientos en Aspera, podría ejecutar comandos en una *shell* restringida *apshell*.

Solución:

IBM ha publicado una serie de parches para solucionar la vulnerabilidad en función del producto afectado. Puede acceder a estos parches en la página de soporte que ha facilitado IBM.

Detalle:

Ciertas aplicaciones Aspera son vulnerables a un desbordamiento de búfer, un atacante remoto, con conocimientos en Aspera, podría realizar una ejecución de comandos en una *shell* restringida *apshell*. Se ha reservado el identificador CVE-2020-4356 para esta vulnerabilidad

Etiquetas: Actualización, IBM, Vulnerabilidad

Omisión de restricción de acceso remoto en productos HPE

Fecha de publicación: 01/04/2020

Importancia: Alta

Recursos afectados:

- HPE MSA 1040 SAN Storage GL225P001 y anteriores,
- HPE MSA 2040 SAN Storage GL225P001 y anteriores,
- HPE MSA 2042 SAN Storage GL225P001 y anteriores,
- HPE MSA 1050 SAN Storage VE270R001-01 y anteriores,
- HPE MSA 2050 SAN Storage VL270R001-01 y anteriores,
- HPE MSA 2052 SAN Storage VL270R001-01 y anteriores.

Descripción:

HPE ha publicado varias vulnerabilidades de omisión de restricción de acceso remoto en los productos afectados.

Solución:

- HPE MSA 1040, versión del firmware GL225P002-02 o posterior;
- HPE MSA 2040, versión del firmware GL225P002-02 o posterior;
- HPE MSA 2042, versión del firmware GL225P002-02 o posterior;
- HPE MSA 1050, versión del firmware VE270P002-02 o posterior;
- HPE MSA 2050, versión del firmware VL270P002-02 o posterior;
- HPE MSA 2052, versión del firmware VL270P002-02 o posterior.

Detalle:

Se han identificado posibles vulnerabilidades de seguridad de la lógica de sesión y de la reutilización de los tokens de sesión remota en los productos afectados. Se han reservado los identificadores CVE-2019-12001 y CVE-2019-12002 para estas vulnerabilidades.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad en dispositivos DrayTek

Fecha de publicación: 02/04/2020

Importancia: Crítica

Recursos afectados:

- Vigor3900, con versiones de firmware anteriores a la 1.5.1;
- Vigor2960, con versiones de firmware anteriores a la 1.5.1;
- Vigor300B, con versiones de firmware anteriores a la 1.5.1.

Descripción:

DrayTek ha detectado una vulnerabilidad de severidad crítica que afecta a algunos modelos de la familia de routers Vigor. Un atacante remoto podría obtener el control del sistema.

Solución:

- Vigor3900, actualizar a la versión de firmware 1.5.1 o superior;
- Vigor2960, actualizar a la versión de firmware 1.5.1 o superior;
- Vigor300B, actualizar a la versión de firmware 1.5.1 o superior.

Detalle:

Una vulnerabilidad en la interfaz de usuario web (WebUI) del dispositivo podría permitir a un atacante remoto obtener el control del sistema. Se ha asignado el identificador CVE-2020-8515 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Ejecución de comandos como root en IBM Spectrum Scale

Fecha de publicación: 03/04/2020

Importancia: Alta

Recursos afectados:

IBM Spectrum Scale, todas las versiones.

Descripción:

Se ha identificado una vulnerabilidad, de severidad alta, en todas las versiones de IBM Sprectum Scale, que podría permitir a un atacante sin privilegios ejecutar comandos como *root*.

Solución:

- Para versiones desde 5.0.0.0 hasta 5.0.4.2, actualizar a la versión 5.0.4.3.
- Para versiones desde 4.2.0.0 hasta 4.2.3.20, actualizar a la versión 4.2.3.21.

Detalle:

IBM Sprectum Scale podría permitir a un atacante local, sin privilegios, con un conocimiento elevado del entorno, ejecutar comandos como *root*, utilizando unos datos de entrada especialmente diseñados. Se ha reservado el identificador CVE-2020-4273 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Desbordamientos de lectura y escritura en SolarWinds Dameware

Fecha de publicación: 07/04/2020

Importancia: Alta

Recursos afectados:

SolarWinds Dameware, versión 12.1 Hotfix 3.

Descripción:

Una vulnerabilidad de severidad alta, de tipo desbordamiento de lectura y escritura en el búfer, en SolarWinds Dameware, podría provocar una condición de denegación de servicio (DoS).

Solución:

Actualizar el producto afectado a la versión 12.1.1.

Detalle:

Cuando se activa el ajuste *Allow only FIPS Mode* en DWRCS.exe, DWRCRSA.dll se carga para realizar el intercambio de claves ECDH (*Elliptic-curve Diffie-Hellman*). Durante el intercambio de claves, el cliente firma el secreto compartido del ECDH con una clave privada de la EC (*Elliptic Curve*) y envía al servidor, tanto la firma, como la clave pública de la EC, para que el mismo pueda verificar la firma. Dentro del mensaje de intercambio de claves, un atacante remoto, no autenticado, podría especificar un gran valor en el campo *SigPubkeyLen* para provocar una condición de sobrelectura/sobreescritura del búfer en DWRCRSA.dll. Se ha reservado el identificador CVE-2020-5734 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad en Log Analysis de IBM

Fecha de publicación: 07/04/2020

Importancia: Alta

Recursos afectados:

IBM Operations Analytics - Log Analysis, versiones desde la 1.3.1, hasta la 1.3.6.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta. Un atacante local, no autenticado, podría ejecutar comandos en el sistema.

Solución:

Actualizar IBM Operations Analytics - Log Analysys a la versión 1.3.6, para luego aplicar el parche de seguridad.

Detalle:

La vulnerabilidad se debe a la posibilidad de introducir comandos del sistema a través de los parámetros de entrada del usuario.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de contraseña embebida en Dell

EMC Data Protection Advisor

Fecha de publicación: 08/04/2020

Importancia: Alta

Recursos afectados:

Dell EMC Data Protection Advisor, versiones 6.4, 6.5 y 18.1.

Descripción:

DEVCORE ha reportado a Dell EMC una vulnerabilidad de credencial embebida en el producto Data Protection Advisor.

Solución:

El fabricante recomienda actualizar el producto afectado a las versiones 18.2, 19.1 o 19.2 para solucionar esta vulnerabilidad.

Detalle:

Múltiples versiones de Dell EMC Data Protection Advisor presentan una vulnerabilidad de credencial embebida en una cuenta no documentada, con privilegios limitados. Un atacante remoto, no autenticado, con el conocimiento de la contraseña embebida, podría ingresar al sistema y obtener privilegios de sólo lectura. Se ha reservado el identificador CVE-2020-5351 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Acceso a información confidencial en vCenter Server de VMware

Fecha de publicación: 13/04/2020

Importancia: Crítica

Recursos afectados:

VMware vCenter Server, versión 6.7, ejecutandose en dispositivos virtuales o Windows.

Descripción:

VMware ha detectado una vulnerabilidad, de severidad crítica, que podría permitir a un atacante remoto revelar información confidencial.

Solución:

Aplicar el parche de seguridad 6.7u3f.

Detalle:

En determinadas condiciones, *vmdir* (VMware Directory Service), que se encuentra incluido en VMware vCenter Server, como parte embebida o externa de un Platform Service Controller (PSC), no implementa correctamente los controles de acceso, pudiendo permitir a un atacante remoto revelar información confidencial. Se ha asignado el identificador CVE-2020-3952 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos Dell EMC

Fecha de publicación: 13/04/2020

Importancia: Alta

Recursos afectados:

- Dell EMC Data Protection Advisor, versiones 6.4, 6.5 y 18.1;
- Dell EMC Isilon OneFS, versón 8.2.2 y anteriores.

Descripción:

Se han publicado dos vulnerabilidades en productos Dell EMC del tipo inyección de comandos en el sistema operativo y configuración por defecto insegura que podrían permitir a un atacante el acceso como administrador o comprometer el sistema.

Solución:

- Actualizar a Dell EMC Data Protection Advisor, versiones 18.2, 19.1 o 19.2;
- Para Dell EMC Isilon OneFS, versión 8.2.2 y anteriores:
  - deshabilitar NFS,
  - mover el directorio admin home,
  - habilitar la autenticación Kerberos,
  - quitar los privilegios SSH (si sólo se utiliza la interfaz de administración web OneFS).

Detalle:

- La vulnerabilidad de inyección de comandos del sistema operativo podría permitir a un atacante remoto, autenticado, ejecutar comandos arbitrarios en el sistema afectado. Se ha reservado el identificador CVE-2020-5352 para esta vulnerabilidad.
- La configuración por defecto de Dell Isilon OneFS, para el Sistema de Archivos en Red (NFS), podría permitir a un atacante acceder a un directorio de inicio 'admin' y, mediante un identificador único (UID) falso a través de NFS, podría reescribir archivos confidenciales con el fin de obtener acceso administrativo al sistema. Se ha reservado el identificador CVE-2020-5353 para esta

vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en IBM WebSphere Application Server

Fecha de publicación: 13/04/2020

Importancia: Alta

Recursos afectados:

IBM WebSphere Application Server, versiones 7.0, 8.0, 8.5 y 9.0.

Descripción:

IBM WebSphere Application Server contiene una vulnerabilidad, de severidad alta, de tipo escalada de privilegios.

Solución:

Para WebSphere Application Server traditional y WebSphere Application Server Hypervisor Edition, aplicar las siguientes medidas, según la versión afectada:

- Desde la 9.0.0.0, hasta la 9.0.5.3, existen dos opciones:
  - actualizar según los requisitos del *interim fix* y luego aplicar el *Interim Fix* PH23853,
  - aplicar el Fix Pack 9.0.5.4 o posterior (disponible en el segundo cuatrimestre de 2020).
- Desde la 8.5.0.0, hasta la 8.5.5.17, existen dos opciones:
  - actualizar según los requisitos del *interim fix* y luego aplicar el *Interim Fix* PH23853,
  - aplicar el Fix Pack 8.5.5.18 o posterior (disponible en el tercer cuatrimestre de 2020).
- Desde la 8.0.0.0, hasta la 8.0.0.15: actualizar a la 8.0.0.15 y luego aplicar el *Interim Fix* PH23853.
- Desde la 7.0.0.0, hasta la 7.0.0.45: actualizar a la 7.0.0.45 y luego aplicar el *Interim Fix* PH23853.

Detalle:

IBM WebSphere Application Server es vulnerable a una escalada de privilegios cuando se utiliza la autenticación basada en *token* en una solicitud de administrador a través del conector SOAP (*Simple Object Access Protocol*). Se ha asignado el identificador CVE-2020-4362 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de Palo Alto Networks

Fecha de publicación: 13/04/2020

Importancia: Alta

Recursos afectados:

- Secdo, todas las versiones para Windows;
- GlobalProtect Agent, versiones anteriores a la 5.0.8 y la 5.1.1 para Linux ARM;
- PAN-OS, versiones:
  - anteriores a la 8.1.13 y la 9.0.7;
  - anteriores a la 9.0.7 en las series PA-7000 con LFC.
- Traps, versiones anteriores a la 5.0.8 y la 6.1.4 para Windows.

Descripción:

Se han publicado múltiples vulnerabilidades en productos de Palo Alto Networks, que podrían permitir a un atacante escalar privilegios, acceder como *root*, ejecutar código como *root*, sobreescribir archivos del sistema o la denegación del servicio.

Solución:

- Secdo carece de soporte. Los problemas pueden ser completamente mitigados:
  - asegurando que los usuarios sin privilegios no tengan acceso a "crear carpeta" en la raíz del sistema de archivos como C: o en una carpeta llamada C:Common,
  - cambiando el permiso en la carpeta C:N-ProgramdataN-SecdoN-Logs para no permitir el acceso a usuarios sin privilegios.
- Actualizar a GlobalProtect Agent 5.0.8, 5.1.1 o versiones posteriores.
- Actualizar a PAN-OS 8.1.13, 9.0.7, 9.1.2 o versiones posteriores.
- Actualizar a Traps 5.0.8, 6.1.4 o versiones posteriores.

Detalle:

- Secdo intenta ejecutar un *script* en una ruta de código, esto podría permitir a un usuario local, autentificado, acceder a la raíz del disco del sistema operativo (C:), mediante 'crear carpetas o añadir datos', para obtener privilegios del sistema si la ruta no existe o si se permite la escritura en ella. Se ha asignado el identificador CVE-2020-1984 para esta vulnerabilidad.
- En Secdo, los permisos por defecto incorrectos en la carpeta C:ProgramdataSecdoN-Logs, podría permitir a los usuarios locales, autentificados, sobrescribir los archivos de sistema y obtener la escalada de privilegios. Se ha asignado el identificador CVE-2020-1985 para esta vulnerabilidad.
- La asignación inadecuada de privilegios cuando se escriben archivos específicos de la aplicación en el Agente GlobalProtect, podría permitir a un usuario local, autentificado, obtener privilegios de *root* en el sistema. Se ha asignado el identificador CVE-2020-1989 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en pila en el componente de servidor de gestión de PAN-OS, podría permitir a un usuario autentificado subir una configuración de PAN-OS corrupta y ejecutar código con privilegios de *root*. Se ha

asignado el identificador CVE-2020-1990 para esta vulnerabilidad.
- Una vulnerabilidad de archivo temporal inseguro en Traps, podría permitir a un usuario local, autentificado, escalar privilegios o sobrescribir archivos de sistema. Se ha asignado el identificador CVE-2020-1991 para esta vulnerabilidad
- Una vulnerabilidad de cadena de formato en el demonio *Varrcvr* de PAN-OS, en dispositivos de la serie PA-7000 con una tarjeta de reenvío de registros (LFC, *Log Forwarding Card*), podría permitir a los atacantes remotos bloquear el demonio creando una condición de negación de servicio o ejecutar potencialmente código con privilegios de *root*. Se ha asignado el identificador CVE-2020-1992 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Intel de abril de 2020

Fecha de publicación: 15/04/2020

Importancia: Alta

Recursos afectados:

- Intel® Modular Server MFS2600KISPP Compute Module, todas las versiones;
- Intel® NUC 8 Rugged Kit NUC8CCHKR;
- Intel® NUC Board NUC8CCHB;
- Intel® NUC 7 Essential PC NUC7CJYSAL;
- Intel® NUC Kit NUC7CJYH
- Intel® NUC Kit NUC7PJYH;
- Intel® NUC Kit NUC6CAYS;
- Intel® NUC Kit NUC6CAYH;
- Intel® NUC Kit DE3815TYKHE;
- Intel® NUC Board DE3815TYBE;
- Intel® Compute Stick STCK1A32WFC.

Descripción:

Los investigadores Michael N. Henry, de DCG Red Team, y Dmitry Frolov han reportado 4 vulnerabilidades, 2 de severidad alta y 2 medias, que permitirían a un atacante realizar una escalada de privilegios o una denegación de servicio.

Solución:

- Para Intel® Modular Server MFS2600KISPP Compute Module, el fabricante recomienda dejar de utilizar el producto, ya que se encuentra descontinuado.
- Para Intel® NUC e Intel® Compute Stick, actualizar el *firmware* a la última versión, tal y como aparece descrito en la tabla *Affected Products* del aviso.

Detalle:

- La comprobación inadecuada de condiciones en Intel(R) Modular Server MFS2600KISPP Compute Module puede permitir a un atacante adyacente, no autenticado, habilitar la escalada de privilegios. Se ha reservado el identificador CVE-2020-0578 para esta vulnerabilidad.
- Unas restricciones inadecuadas de búfer en el *firmware* para algunos Intel(R) NUC pueden permitir a un atacante local, autenticado, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2020-0600 para esta vulnerabilidad.

Para las vulnerabilidades de severidad media, se han reservado los identificadores CVE-2020-0576 y CVE-2020-0577.

Etiquetas: Actualización, Vulnerabilidad

Boletín de seguridad de Microsoft de abril de 2020

Fecha de publicación: 15/04/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge (basado en Chromium);
- ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Windows Defender;
- Visual Studio;
- Microsoft Dynamics;
- Microsoft Apps para Android;
- Microsoft Apps para Mac.

Impacto:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de abril, consta de 112 vulnerabilidades, 17 clasificadas como críticas y 95 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.

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*),
- evasión de restricciones de seguridad.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Actualizaciones críticas en Oracle (abril 2020)

Fecha de publicación: 15/04/2020

Importancia: Crítica

Recursos afectados:

- Application Performance Management, versiones 12.1.0.5, 13.2.0.0, 13.3.0.0;
- Application Service Level Management, versiones 13.2.0.0, 13.3.0.0;
- Enterprise Manager Base Platform, versiones 12.1.0.5, 13.2.0.0, 13.3.0.0;
- Hyperion Financial Management, versión 11.1.2.4;
- Hyperion Financial Reporting, versión 11.1.2.4;
- Identity Manager Connector, versión 9.0;
- Instantis EnterpriseTrack, versiones 17.1-17.3;
- Java Advanced Management Console, versión 2.16;
- JD Edwards EnterpriseOne Tools, versión 9.2;
- JD Edwards World Security, versiones A9.3, A9.3.1, A9.4;
- MICROS Relate CRM Software, versión 11.4;
- MySQL Client, versiones 5.6.47 y anteriores, 5.7.29 y anteriores, 8.0.18 y anteriores;
- MySQL Cluster, versiones 7.3.28 y anteriores, 7.4.27 y anteriores, 7.5.17 y anteriores, 7.6.13 y anteriores, 8.0.19 y anteriores;
- MySQL Connectors, versiones 5.1.48 y anteriores, 8.0.19 y anteriores;
- MySQL Enterprise Monitor, versiones 4.0.11.5331 y anteriores, 8.0.18.1217 y anteriores;
- MySQL Server, versiones 5.6.47 y anteriores, 5.7.29 y anteriores, 8.0.19 y anteriores;
- MySQL Workbench, versiones 8.0.19 y anteriores;
- Oracle Access Manager, versiones 11.1.2.3.0, 12.2.1.3.0;
- Oracle Agile PLM, versiones 9.3.3, 9.3.5, 9.3.6;
- Oracle API Gateway, versión 11.1.2.4.0;
- Oracle Application Express, versiones anteriores a la 19.2;
- Oracle Application Testing Suite, versiones 13.2.0.1, 13.3.0.1;
- Oracle Banking Enterprise Collections, versiones 2.7.0, 2.8.0;
- Oracle Banking Enterprise Originations, versiones 2.7.0, 2.8.0;
- Oracle Banking Enterprise Product Manufacturing, versiones 2.7.0, 2.8.0;
- Oracle Banking Platform, versiones 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, 2.9.0;
- Oracle Big Data Discovery, versión 1.6;
- 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, versión 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;
- Oracle Communications ASAP Cartridges, versiones 7.2, 7.3;
- Oracle Communications Calendar Server, versiones 8.0.0.2.0, 8.0.0.3.0;
- Oracle Communications Converged Application Server - Service Controller, versión 6.1;
- Oracle Communications Diameter Signaling Router (DSR), versiones 8.0.0, 8.1.0, 8.2.0, 8.2.1;
- Oracle Communications Element Manager, versiones 8.0.0, 8.1.0, 8.1.1, 8.2.0;
- Oracle Communications Evolved Communications Application Server, versión 7.1;
- Oracle Communications Messaging Server, versiones 8.0.2, 8.1.0;
- Oracle Communications Operations Monitor, versiones 3.4.0, 4.0.0, 4.1.0, 4.2.0, 4.3.0;
- Oracle Communications Service Broker, versiones 6.0, 6.1;
- Oracle Communications Services Gatekeeper, versiones 6.0, 6.1;
- Oracle Communications Session Report Manager, versiones 8.0.0, 8.1.0, 8.1.1, 8.2.0;
- Oracle Communications Session Route Manager, versiones 8.0.0, 8.1.0, 8.1.1, 8.2.0;
- Oracle Communications Unified Inventory Management, versiones 7.3.0, 7.4.0;
- Oracle Communications WebRTC Session Controller, versión 7.2;
- Oracle Configurator, versiones 12.1, 12.2;
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c;
- 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 Server, versión 7.7.0;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 8.0.6-8.0.9;
- Oracle Financial Services Asset Liability Management, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Balance Sheet Planning, versión 8.0.8;
- Oracle Financial Services Data Foundation, versiones 8.0.6-8.0.9;
- Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management, versiones 8.0.7, 8.0.8;
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Hedge Management and IFRS Valuations, versiones 8.0.6-8.0.8;
- Oracle Financial Services Liquidity Risk Management, versión 8.0.6;
- Oracle Financial Services Liquidity Risk Measurement and Management, versiones 8.0.7, 8.0.8;
- Oracle Financial Services Loan Loss Forecasting and Provisioning, versiones 8.0.6-8.0.8;
- Oracle Financial Services Market Risk Measurement and Management, versiones 8.0.6, 8.0.8;
- Oracle Financial Services Price Creation and Discovery, versión 8.0.7;
- Oracle Financial Services Profitability Management, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Revenue Management and Billing Analytics, versiones 2.6, 2.7, 2.8;
- Oracle FLEXCUBE Core Banking, versión 4.0;
- Oracle FLEXCUBE Private Banking, versiones 12.0, 12.1;
- Oracle Fusion Middleware MapViewer, versión 12.2.1.3.0;
- Oracle Global Lifecycle Management NextGen OUI Framework, versiones 12.2.1.3.0, 12.2.1.4.0, 13.9.4.2.2;
- Oracle Global Lifecycle Management OPatch, versiones anteriores a la 11.2.0.3.23, anteriores a la 12.2.0.1.19, anteriores a la 13.9.4.2.1;
- Oracle GraalVM Enterprise Edition, versiones 19.3.1, 20.0.0;
- Oracle Health Sciences Information Manager, versión 3.0;
- Oracle Healthcare Data Repository, versión 7.0;

- Oracle Hospitality Reporting and Analytics, versión 9.1.0;
- Oracle HTTP Server, versión 11.1.1.9.0;
- Oracle In-Memory Performance-Driven Planning, versiones 12.1, 12.2;
- Oracle Insurance Accounting Analyzer, versiones 8.0.6-8.0.9;
- Oracle Java SE, versiones 7u251, 8u241, 11.0.6, 14;
- Oracle Java SE Embedded, versión 8u241;
- Oracle Knowledge, versiones 8.6.0-8.6.3;
- Oracle Managed File Transfer, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Outside In Technology, versiones 8.5.4, 8.5.5;
- Oracle Real User Experience Insight, versiones 13.1.2.1, 13.2.3.1, 13.3.1.0;
- Oracle Retail Advanced Inventory Planning, versiones 14.0, 15.0, 16.0;
- Oracle Retail Back Office, versión 14.1;
- Oracle Retail Central Office, versión 14.1;
- Oracle Retail Customer Management and Segmentation Foundation, versión 18.0;
- Oracle Retail Merchandising System, versión 16.0;
- Oracle Retail Order Broker, versiones 15.0, 16.0, 18.0, 19.0;
- Oracle Retail Point-of-Service, versión 14.1;
- Oracle Retail Predictive Application Server, versiones 15.0.3, 16.0.3;
- Oracle Retail Returns Management, versión 14.1;
- Oracle Retail Store Inventory Management, versión 16.0;
- Oracle Retail Xstore Point of Service, versiones 7.1, 15.0, 16.0, 17.0, 18.0, 18.0.1;
- Oracle SD-WAN Edge, versiones 7.3, 8.0, 8.1, 8.2;
- Oracle Secure Backup, versiones anteriores a la 18.1;
- Oracle SOA Suite, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Solaris, versiones 10, 11;
- Oracle Transportation Management, versiones 6.3.7, 6.4.2, 6.4.3;
- Oracle Unified Directory, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Utilities Framework, versiones 2.2.0, 4.2.0.2, 4.2.0.3, 4.3.0.2-4.3.0.6, 4.4.0.0, 4.4.0.2;
- Oracle Utilities Network Management System, versiones 1.12.0.3, 2.3.0.1, 2.3.0.2, 2.4.0.0;
- Oracle VM VirtualBox, versiones anteriores a la 5.2.40, anteriores a la 6.0.20, anteriores a la 6.1.6;
- 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;
- OSS Support Tools, versiones 20.0, 20.1;
- PeopleSoft Enterprise CS Campus Community, versión 9.2;
- PeopleSoft Enterprise HCM Absence Management, versión 9.2;
- PeopleSoft Enterprise HRMS, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57, 8.58;
- PeopleSoft Enterprise SCM Purchasing, versión 9.2;
- Primavera Gateway, versiones 16.2.0-16.2.11, 17.12.0-17.12.6, 18.8.0-18.8.8, 19.12.0;
- Primavera P6 Enterprise Project Portfolio Management, versiones 16.2.0.0-16.2.19.3, 17.12.0.0-17.12.17.0, 18.8.0.0-18.8.18.0, 19.12.1.0-19.12.3.0, 20.1.0.0-20.2.0.0;
- Primavera Unifier, versiones 16.1, 16.2, 17.7-17.12, 18.8, 19.12;
- Siebel Applications, versiones 20.2 y anteriores;
- StorageTek Tape Analytics SW Tool, versión 2.3.0;
- Sun ZFS Storage Appliance Kit, versión 8.8.

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 397 vulnerabilidades, algunas de las cuales son críticas. El detalle de las vulnerabilidades resueltas se puede consultar en el enlace de Oracle de la sección de *Referencias*.

Etiquetas: Actualización, Oracle, Vulnerabilidad

Múltiples vulnerabilidades en ClearPass Policy Manager de Aruba

Fecha de publicación: 15/04/2020

Importancia: Crítica

Recursos afectados:

- ClearPass Policy Manager, versiones 6.8.x, anteriores a la versión 6.8.4;
- ClearPass Policy Manager, versiones 6.7.x, anteriores a la versión 6.7.13.

Descripción:

Los investigadores, Luke Young, Sathish y Darrell Damstedt, han reportado a Aruba 4 vulnerabilidades, una de severidad crítica, una de severidad alta y dos de severidad media. Un atacante remoto, no autenticado, podría ejecutar código arbitrario, realizar una escalada de privilegios, revelar información confidencial o evadir las restricciones de seguridad y comprometer el *cluster*.

Solución:

- Actualizar ClearPass Policy Manager, versiones 6.8.x, a la versión 6.8.4;
- Actualizar ClearPass Policy Manager, versiones 6.7.x, a la versión 6.7.13;

Detalle:

- La vulnerabilidad de severidad crítica podría permitir a un atacante, que se encuentre en el mismo segmento de red que el de la interfaz de gestión de ClearPass, realizar cambios en algunas bases de datos de ClearPass mediante el envío de peticiones HTTP

especialmente generadas. Pudiendo comprometer completamente el *cluster*. Se ha reservado el identificador CVE-2020-7114 para esta vulnerabilidad.
- La vulnerabilidad de criticidad alta se debe a la existencia de una inyección en el lado del servidor que podría permitir a un atacante, autenticado, realizar una ejecución remota de código. Se ha reservado el identificador CVE-2020-7111 para esta vulnerabilidad.
- A las vulnerabilidades de severidad media se les han reservado los identificadores CVE-2020-7110 y CVE-2020-7113.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de abril de 2020

Fecha de publicación: 15/04/2020

Importancia: Crítica

Recursos afectados:

- SAP Commerce, versiones 6.6, 6.7, 1808, 1811 y 1905;
- SAP Diagnostic Agent (LM-Service), versión 7.20;
- SAP NetWeaver:
  - Knowledge Management, versiones 7.00, 7.01, 7.02, 7.30, 7.31, 7.40 y 7.50;
  - AS (Application Server) Java (HTTP Service), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
  - AS ABAP, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 75A, 75B, 75C, 75D y 75E;
- SAP Business Objects Business Intelligence Platform, versiones 4.1, 4.2 y 4.3;
- SAP OrientDB, versión 3.0;
- SAP Solution Manager (Diagnostics Agent), versión 7.2;
- SAP Host Agent, versión 7.21;
- SAP Landscape Management, versión 3.0;
- SAP Adaptive Extensions, versión 1.0;
- SAP ERP, versiones 618, 730 y EAPPLGLO 607 ;
- SAP S/4 HANA, versiones 100, 101, 102, 103, 104, FSAPPL 400, 450, 500 y S4FPSL 100;
- SAP Business Client, versiones 6.5 y 7.0 ;
- SAP Commerce, versiones 1811 y 1905;
- SAP Fiori Launchpad, versiones 753 y 754.

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 26 notas de seguridad, de las cuales 5 son de severidad crítica, 5 de severidad alta y 16 de severidad media. Además, se incluyen 3 actualizaciones de notas de seguridad publicadas con anterioridad, incluidas dentro de las 26 totales (2 corresponden a severidad crítica y 1 a media).

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 11 vulnerabilidades de XSS (*Cross-Site Scripting*),
- 4 vulnerabilidades de divulgación de información,
- 3 vulnerabilidades de falta de comprobación de autenticación,
- 2 vulnerabilidades de inyección de código,
- 2 vulnerabilidades de redirección de URL,
- 1 vulnerabilidad de acceso a rutas no controlado,
- 1 vulnerabilidad de falta de autenticación,
- 1 vulnerabilidad de falta de validación de XML,
- 8 vulnerabilidades de otro tipo.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-6238, CVE-2019-0330, CVE-2020-6225, CVE-2020-6219, CVE-2020-6230, CVE-2020-6235, CVE-2020-6208, CVE-2020-6237, CVE-2020-6234, CVE-2020-6236, CVE-2020-6195, CVE-2020-6212, CVE-2020-6224, CVE-2020-6216, CVE-2020-6215, CVE-2020-6213, CVE-2020-6217, CVE-2020-6229, CVE-2020-6226, CVE-2020-6231, CVE-2020-6222, CVE-2020-6228, CVE-2020-6227, CVE-2020-6232, CVE-2020-6210, CVE-2020-6214 y CVE-2020-6233.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en IBM QRadar SIEM

Fecha de publicación: 15/04/2020

Importancia: Alta

Recursos afectados:

IBM QRadar, desde la versión 7.3.0, hasta la 7.3.3 Patch 2;

Descripción:

Los permisos de archivo incorrectos y las credenciales embebidas en IBM QRadar SIEM, podrían permitir a un atacante la escalada de privilegios o el uso de dichas credenciales.

Solución:

Aplicar las actualizaciones:

- QRadar / QRM / QVM / QNI 7.4.0 GA (SFS);
- QRadar / QRM / QVM / QRIF / QNI 7.3.3 Patch 3 (SFS);
- QRadar / QRM / QVM / QRIF / QNI 7.3.2 Patch 7(SFS);
- QRadar Incident Forensics 7.4.0 (ISO);
- QRadar Incident Forensics 7.4.0 (SFS).

Detalle:

- Los permisos de archivo incorrectos podrían permitir a un atacante la escalada de privilegios. Se ha reservado el identificador CVE-2020-4270 para esta vulnerabilidad.
- La presencia de credenciales embebidas, como una contraseña o clave criptográfica, que es usada para su propia autenticación de entrada, comunicación saliente hacia componentes externos o cifrado de datos internos, podría permitir a un atacante utilizar dichas credenciales. Se ha reservado el identificador CVE-2020-4269 para esta vulnerabilidad

Etiquetas: Actualización, IBM, Vulnerabilidad

Inyección de comandos en Integrated Data Protection Appliance de Dell EMC

Fecha de publicación: 15/04/2020

Importancia: Alta

Recursos afectados:

- Dell EMC Integrated Data Protection Appliance, versiones 2.0, 2.1, 2.2, 2.3 y 2.4.

Descripción:

Dell EMC ha detectado una vulnerabilidad de severidad alta que afecta a Integrated Data Protection Appliance.

Solución:

Actualizar Dell EMC Integrated Data Protection Appliance a la versión 2.5.

Los usuarios que dispongan de la versión Integrated Data Protection Appliance 2.0, deberán actualizar previamente a la versión 2.1, luego a la versión 2.3.1, y finalmente a la 2.5.

Detalle:

Existe una vulnerabilidad de inyección de comandos en el componente Appliance Configuration Manager. Un atacante remoto, autenticado, con privilegios de *root,* podría inyectar comandos en la API de ese componente, y de este modo, modificar contraseñas y ejecutar comandos. Se ha reservado el identificador CVE-2020-5350 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 16/04/2020

Importancia: Crítica

Recursos afectados:

- IP Phone 7811, 7821, 7841, 7861, 8811, 8841, 8845, 8851, 8861 y 8865 Desktop Phones;
- Unified IP Conference Phone 8831;
- Wireless IP Phone 8821 y 8821-EX;
- Cisco UCS Director, versiones 6.0.0.0, 6.0.0.1, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.0.1.3, 6.5.0.0, 6.5.0.1, 6.5.0.2, 6.5.0.3, 6.5.0.4, 6.6.0.0, 6.6.1.0, 6.6.2.0, 6.7.0.0, 6.7.1.0, 6.7.2.0 y 6.7.3.0;
- Cisco UCS Director Express para Big Data, versiones 3.7.3.0 y anteriores;
- dispositivos Cisco si están ejecutando una versión vulnerable de Cisco WLC Software;
- Cisco Access Points (AP) que actúan como controladores Mobility Express si están ejecutando una versión vulnerable de Cisco WLC Software;
- Cisco Webex Meetings, todas la versiones Webex Network Recording Player y Webex Player anteriores a WBS 39.5.18 o WBS 40.2;
- Cisco Webex Meetings Online, todas la versiones Webex Network Recording Player y Webex Player anteriores a 1.3.48;
- Cisco Webex Meetings Server, todas las versiones Webex Network Recording Player anteriores a 4.0MR3;
- Aironet 1540/1560/1800/2800/3800/4800 Series Access Points;
- Catalyst IW6300 Access Points;
- 6300 Embedded Services Access Points;
- Cisco IoT Field Network Director, versiones anteriores a 4.6;
- Cisco Unified Communications Manager (UCM) y Cisco UCM Session Management Edition (SME), versiones 10.5 y anteriores, 11.0, 11.5, 12.0 y 12.5, cuando la funcionalidad *auto-registration* está activada.

Descripción:

Diversos investigadores han descubierto 18 vulnerabilidades, 11 de severidad crítica y 7 altas, de tipo ejecución remota de código, denegación de servicio, omisión de autenticación, acceso a directorios no controlado, desbordamiento de búfer y *Cross-Site Request Forgery*.

Solución:

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

Detalle:

Un atacante que aprovechase estas vulnerabilidades podría realizar alguna de las siguientes acciones:

- reiniciar el dispositivo afectado, generando una condición de denegación de servicio (DoS);
- ejecutar comandos arbitrarios con privilegios de administrador;
- realizar llamadas a la API;
- ejecutar código arbitrario en el sistema afectado;
- leer, modificar o ejecutar archivos arbitrarios con permisos de *root*;
- realizar acciones arbitrarias, como modificar la configuración, con el nivel de privilegios del usuario afectado;
- bloquear el *access point* (AP), generando una condición de denegación de servicio (DoS).

Se han asignado los siguientes identificadores: CVE-2020-3161, CVE-2020-3239, CVE-2020-3240, CVE-2020-3243, CVE-2020-3247, CVE-2020-3248, CVE-2020-3249, CVE-2020-3250, CVE-2020-3251, CVE-2020-3252, CVE-2016-1421, CVE-2020-3273, CVE-2020-3262, CVE-2020-3194, CVE-2020-3261, CVE-2020-3162, CVE-2020-3177 y CVE-2020-3260.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Escalada de privilegios en InfoSphere Information Server de IBM

Fecha de publicación: 16/04/2020

Importancia: Alta

Recursos afectados:

- InfoSphere Information Server, Information Server on Cloud, versiones 11.7 y 11.5;
- InfoSphere Information Server, versión 11.3.

Cuyas instalaciones cumplan las siguientes condiciones:

- Utiliza Information Server, versión 11.7.1. o anterior, o si se actualizó dicha instalación a una versión posterior a la 11.7.1.0.
- Utiliza WebSphere Application Server Network Deployment (WAS ND).
- Fue instalado utilizando *umask* más débil que 022.

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta que afecta a InfoSphere Information Server. Un atacante remoto podría realizar una escalada de privilegios.

Solución:

- Para sistemas desplegados independientemente:
  - En la ubicación de WAS ND, cambiar el directorio por el que contiene la carpeta java.
  - chmod -R 755 java.
- Para sistemas desplegados en clústeres:
  - En la máquina donde esté instalado el gestor:
    - En la ubicación de WAS ND, cambiar el directorio por el que contiene la carpeta java.
    - chmod -R 755 java.
  - En la máquina donde se instaló un perfil personalizado (realizar en todas las máquinas que dispongan de un perfil personalizado, o máquinas horizontales que pertenezcan al clúster):
    - En la ubicación de WAS ND, cambiar el directorio por el que contiene la carpeta java.
    - chmod -R 755 java.

Detalle:

IBM InfoSphere Information Server podría ser susceptible a ataques basados en escalada de privilegios, debido a una asignación inapropiada de permisos en los archivos utilizados por WebSphere Application Server Network Deployment. Se ha reservado el identificador CVE-2020-4347 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Vulnerabilidad de fallo de segmentación en SSL_check_chain de OpenSSL

Fecha de publicación: 22/04/2020

Importancia: Alta

Recursos afectados:

OpenSSL, versiones 1.1.1d, 1.1.1e y 1.1.1f

Descripción:

Los investigadores Bernd Edlinger, Matt Caswell y Benjamin Kaduk reportaron a OpenSSL una vulnerabilidad localizada en la función *SSL_check_chain()*, con severidad alta y de tipo fallo de segmentación.

Solución:

Actualizar OpenSSL a la versión 1.1.1g.

Detalle:

Las aplicaciones de servidor o cliente que invocan a la función *SSL_check_chain()*, durante o después de un *handshake* TLS 1.3, podrían bloquearse debido a una desreferencia del puntero NULL, como resultado del manejo incorrecto de la extensión TLS

signature_algorithms_cert. El bloqueo podría producirse si se recibe un algoritmo de firma no válido o no reconocido del par, pudiendo ser utilizado para realizar un ataque de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-1967 para esta vulnerabilidad.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.18

Fecha de publicación: 22/04/2020

Importancia: Baja

Recursos afectados:

- Joomla! CMS, versiones:
  - desde la 3.8.8, hasta la 3.9.16;
  - desde la 2.5.0, hasta la 3.9.16.

Descripción:

Joomla! ha publicado dos nuevas versiones que solucionan 3 vulnerabilidades de criticidad baja en su núcleo, todas ellas del tipo control de acceso incorrecto.

Joomla! desaconseja actualizar a la versión 3.9.17 y recomienda actualizar directamente a la versión 3.9.18.

Solución:

Actualizar a la versión 3.9.18.

Detalle:

- Una incorrecta comprobación de *com_users* en las Listas de Control de Acceso (ACL), podría permitir a un atacante no autorizado editar el grupo de usuarios. Se ha asignado el CVE-2020-11891 para esta vulnerabilidad.
- Una incorrecta validación de los parámetros de entrada en la clase tabla del grupo de usuarios podría romper la configuración de las ACL. Se ha asignado el CVE-2020-11890 para esta vulnerabilidad.
- Una incorrecta comprobación de *com_users* en las ACL, podría permitir a un atacante no autorizado eliminar el grupo de usuarios. Se ha asignado el CVE-2020-11889 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de puerto UDP abierto en múltiples productos de HPE

Fecha de publicación: 24/04/2020

Importancia: Alta

Recursos afectados:

- Integrated Maintenance Entity T1805, versiones desde T1805A01 hasta T1805A01^AAH;
- Maintenance Entity T2805, versiones desde T2805A01 hasta T2805A01^AAU;
- Blade Maintenance Entity FW T4805, versiones desde T4805A01 hasta T4805A01^AAY.

Descripción:

HPE Product Security Response Team ha detectado una vulnerabilidad, de severidad alta, asociada a un puerto UDP abierto, que permitiría a un atacante realizar una denegación de servicio, divulgar información o corromper la memoria de los productos afectados.

Solución:

- Integrated Maintenance Entity, actualizar a la versión T1805A01^AAI;
- Blade Maintenance Entity, actualizar a la versión T4805A01^AAZ.

Como medida de mitigación, se puede bloquear el puerto UDP 17185 en Maintenance LAN Network Switch/Firewall.

Detalle:

Todos los sistemas NonStop de la serie J/H tienen una vulnerabilidad de seguridad asociada con el puerto UDP 17185 abierto en la Maintenance LAN, que podría provocar que un atacante remoto realizara una divulgación de información, ataques de denegación de servicio (DoS) o corrompiera la memoria local, obteniendo un control total del sistema afectado. Se ha reservado el identificador CVE-2020-7131 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Vulnerabilidad en BIG-IQ Centralized Management de F5

Fecha de publicación: 24/04/2020

Importancia: Alta

Recursos afectados:

BIG-IQ Centralized Management, versiones 7.0.0, 6.0.0 - 6.1.0, 5.2.0 - 5.4.0.

Descripción:

Se ha publicado una vulnerabilidad que podría permitir a un atacante comprometer ciertos datos del BIG-IQ cuando se explota en una configuración BIG-IQ HA.

Solución:

Actualizar a la versión 7.1.0.

Detalle:

La sincronización de alta disponibilidad (HA) de BIG-IQ no es segura por TLS, lo que podría permitir a un atacante leer/modificar los datos confidenciales en tránsito. Se ha reservado el identificador CVE-2020-5869 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 24/04/2020

Importancia: Crítica

Recursos afectados:

- IBM Spectrum Protect Server, versiones:
  - desde 8.1.0.0, hasta 8.1.9.200;
  - desde 7.1.0.0, hasta 7.1.10.0.
- IBM Tivoli Monitoring, versiones desde 6.3.0, hasta 630 FP7 (incluyendo *service packs*).

Descripción:

Los investigadores, Chris Lyne, de Tenable, y Clément Notin han notificado dos vulnerabilidades a IBM, de severidad crítica y alta respectivamente, de tipo desbordamiento de búfer y permisos por defecto insuficientes.

Solución:

- Actualizar IBM Spectrum Protect Server a las versiones 8.1.9.300 y 7.1.10.100.
- Actualizar IBM Tivoli Monitoring a la versión 6.3.0-TIV-ITM-FP0007-CVE-2020-4311.

Detalle:

- IBM Spectrum Protect Server es vulnerable a un desbordamiento de búfer basado en la pila (*stack*), que podría permitir a un atacante remoto ejecutar código arbitrario en el sistema o provocar el bloqueo del producto afectado. Se ha asignado el identificador CVE-2020-7131 para esta vulnerabilidad.
- IBM Tivoli Monitoring podría permitir a un atacante local utilizar un archivo, especialmente diseñado, para cargar otros archivos DLL ubicados en el mismo directorio y, de esta manera, ejecutar código arbitrario en el producto afectado. Se ha asignado el identificador CVE-2020-4311 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de desbordamiento de enteros en Squid

Fecha de publicación: 24/04/2020

Importancia: Alta

Recursos afectados:

- Squid 2.x - 2.7.STABLE9;
- Squid 3.x - 3.5.28;
- Squid 4.x - 4.10;
- Squid 5.x - 5.0.1.

Descripción:

Debido a un error de desbordamiento de números enteros, el servidor proxy Squid es vulnerable a la repetición de credenciales y a los ataques de ejecución de código remoto contra los tokens de autenticación de HTTP Digest.

Solución:

Actualizar a la versión 4.11 o 5.0.2.

Como medida de mitigación, eliminar todas las líneas "auth_param digest" de squid.conf, activar la opción "--disable-auth-digest" o la opción "--disable-auth".

Detalle:

Cuando se utiliza el *pool* de memoria este problema podría permitir a un cliente remoto reproducir una autenticación de Digest previamente interceptada para acceder a recursos que de otra manera estrían prohibidos. Cuando la reserva de memoria está deshabilitada, un cliente remoto podría ejecutar código a través de las credenciales de un "free'd nonce". Se ha asignado el identificador CVE-2020-11945 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de HPE

Fecha de publicación: 27/04/2020

Importancia: Alta

Recursos afectados:

- HPE IOT GCP, versiones 1.4.0, 1.4.1, 1.4.2 y 1.2.4.2;
- HPE Service Pack para ProLiant, versiones 2018.06.0, 2018.09.0 y 2018.11.0 (solo aplica al instalador de firmware de Linux);
- HPE SATA Read Intensive Solid State Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE NVMe Mixed Use Solid State Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE Business Critical Hard Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE Server Enterprise Hard Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE Server SAS Hard Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE Server SATA Hard Drives HPG2 (solo aplica al instalador de *firmware* de Linux);
- HPE Server Solid State Drives HPG2 (solo aplica al instalador de *firmware* de Linux).

Descripción:

Se han detectado 3 vulnerabilidades, 2 de severidad alta y una media, de tipo acceso remoto no autorizado, ejecución de código arbitrario de manera local y acceso remoto a información sensible, respectivamente.

Solución:

- Actualizar HPE UIoT a la versión 1.4.2 RP204.
- Para los productos afectados por la vulnerabilidad CVE-2020-7135, las soluciones que aparecen listadas en la sección *RESOLUTION* del aviso pueden aplicarse actualizando HPE Service Pack para ProLiant a la versión 2019.03.0 o posteriores, o actualizando Online HDD/SDD Flash Component para Linux, ambos disponibles desde la web de HPE Support Center.

Detalle:

- Un atacante remoto, no autorizado, podría obtener acceso a información sensible en varias versiones de HPE UIoT. Se ha asignado el identificador CVE-2020-7133 para esta vulnerabilidad.
- Se ha identificado una vulnerabilidad en los instaladores de *firmware* de la unidad de disco denominados *Supplemental Update / Online ROM Flash Component* en los servidores HPE que ejecutan Linux. Un atacante local podría ejecutar código arbitrario en este *software* vulnerable. Se ha reservado el identificador CVE-2020-7135 para esta vulnerabilidad.

Para la vulnerabilidad de severidad media, se ha asignado el identificador CVE-2020-7134.

Etiquetas: Actualización, HP, Vulnerabilidad

Control de acceso inapropiado en productos de Fortinet

Fecha de publicación: 28/04/2020

Importancia: Crítica

Recursos afectados:

- FortiMail, versiones:
  - 5.4.10 y anteriores;
  - 6.0.7 y anteriores;
  - 6.2.2 y anteriores.
- FortiVoiceEnterprise, versiones:
  - 6.0.1 y anteriores;
  - las versiones 5.3 y anteriores, no se ven afectadas por esta vulnerabilidad.

Descripción:

El investigador Mike Connor ha detectado una vulnerabilidad, de severidad crítica, del tipo control de acceso inapropiado, que afecta a varios productos de Fortinet. Un atacante remoto, no autenticado, podría evadir la autenticación.

Solución:

- Actualizar ForiMail a las versiones:
  - 5.4.11 o posterior;
  - 6.0.8 o posterior;
  - 6.2.3 o posterior.
- Actualizar FortiVoiceEnterprise a la versión 6.0.2 o posterior.

Detalle:

Una vulnerabilidad de control de acceso inapropiado, en FortiMail y FortiVoiceEnterpries, podría permitir a un atacante remoto, no autenticado, acceder al sistema como un usuario legitimo al solicitar un cambio de contraseña a través de la interfaz de usuario. Se ha asignado el identificador CVE-2020-9294 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Acceso no controlado a rutas en Juno OS de Juniper

Fecha de publicación: 28/04/2020

Importancia: Alta

Recursos afectados:

Junos OS, versiones 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4 y 20.1.

Descripción:

Una vulnerabilidad en el servicio HTTP/HTTPS, de severidad alta, utilizado por varios productos de Juniper, permite que un atacante no autenticado realice una inclusión local de archivos (LFI, *Local File Inclusion*) o el acceso no controlado a rutas.

Solución:

Las siguientes versiones de *software* se han publicado para resolver esta vulnerabilidad: 12.3X48-D101, 12.3X48-D105, 15.1X49-D211, 15.1X49-D220, 17.4R3-S2, 18.1R3-S10, 18.2R3-S4, 18.3R2-S4, 18.3R3-S2, 18.4R3-S2, 19.1R1-S5, 19.1R3-S1, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1-S1, 20.1R2 y todas las versiones posteriores, disponibles desde el centro de descargas de Juniper.

Detalle:

El servicio HTTP/HTTPS, que es utilizado por J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through con Web-Redirect y Zero Touch Provisioning (ZTP), contiene una vulnerabilidad que permitiría a un atacante, no autenticado, inyectar comandos en *httpd.log*, leer archivos con permisos globales u obtener *tokens* de sesión J-Web. Se ha reservado el identificador CVE-2020-1631 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de XSS en VMware ESXi

Fecha de publicación: 29/04/2020

Importancia: Alta

Recursos afectados:

VMware ESXi, versiones 6.5 y 6.7.

Descripción:

Benny Husted y DAWUSHI han reportado una vulnerabilidad, de severidad alta, de tipo *Cross-Site Scripting* (XSS) persistente, en varias versiones de VMware ESXi.

Solución:

- VMware ESXi 6.5, actualizar a la versión ESXi650-201912104-SG;
- VMware ESXi 6.7, actualizar a la versión ESXi670-202004103-SG.

Detalle:

VMware ESXi Host Client no neutraliza correctamente el HTML relacionado con las secuencias de comandos cuando se visualizan los atributos de las máquinas virtuales. Un atacante, si tuviera acceso a las propiedades del sistema de una máquina virtual desde el sistema operativo invitado, podría inyectar un *script* malicioso que sería ejecutado por el navegador de la víctima. Se ha asignado el identificador CVE-2020-3955 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Vulnerabilidades en Samba

Fecha de publicación: 29/04/2020

Importancia: Alta

Recursos afectados:

- Todas las versiones de Samba, desde la versión 4.0.0 en adelante;
- Todas las versiones de Samba, desde la versión 4.10.0 en adelante.

Descripción:

Andrew Barlett de Catalyst, y Andrei Popa, han detectado dos vulnerabilidades, una de criticidad alta y otra media, que afectan a múltiples versiones de Samba. Un atacante remoto, no autenticado, podría utilizar memoria previamente liberada (*use-after-free*) u ocasionar un *SIGSEGV* en el servidor.

Solución:

Actualizar a las versiones 4.10.15, 4.11.8 o 4.12.2.

Detalle:

- La vulnerabilidad de severidad alta se debe a una búsqueda LDAP, no autenticada, mediante un filtro profundamente anidado, esto puede agotar los recursos de la pila de memoria del servidor LDAP y ocasionar un *SIGSEGV*. Se ha reservado el identificador CVE-

2020-10704 para esta vulnerabilidad.
- A la vulnerabilidad de severidad media, del tipo uso de memoria previamente liberada (*user-after-free*), se le ha reservado el identificador CVE-2020-10700.

Etiquetas: Actualización, Samba, Vulnerabilidad

Acceso remoto no autorizado en Smart Update Manager de HPE

Fecha de publicación: 30/04/2020

Importancia: Crítica

Recursos afectados:

Smart Update Manager (SUM), versiones anteriores a la 8.5.6.

Descripción:

Se han publicado tres vulnerabilidades de severidad crítica en productos SUM de HPE que podrían permitir el acceso remoto no autorizado.

Solución:

Actualizar a la última versión de SUM desde el centro de soporte de HPE.

Detalle:

Tres vulnerabilidades de severidad crítica en Smart Update Manager de HPE podrían permitir a un atacante el acceso remoto no autorizado. Se han asignado los identificadores CVE-2017-2921 y CVE-2017-2922, y reservado el identificador CVE-2020-7136 para estas vulnerabilidades.

Etiquetas: Actualización, HP, Vulnerabilidad

Inyección de comandos en IOS XE SD-WAN de Cisco

Fecha de publicación: 30/04/2020

Importancia: Alta

Recursos afectados:

Los siguientes dispositivos de Cisco que ejecutan el software IOS XE SD-WAN:

- 1000 Series Aggregation Services Routers,
- 1000 Series Integrated Services Routers (ISRs),
- 4000 Series ISRs,
- Cloud Services Router 1000V Series.

Descripción:

Los investigadores Julien Legras y Thomas Etrillard, de Synacktiv, han detectado una vulnerabilidad de criticidad alta que afecta a varios dispositivos de Cisco. Un atacante local, autenticado, inyectar comandos con privilegios de *root*.

Solución:

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

Detalle:

La vulnerabilidad se debe a una insuficiente validación de los parámetros de entrada. Un atacante local, autenticado, podría introducir una entrada, específicamente generada, en la utilidad CLI, y podría ejecutar comandos en el dispositivo con privilegios de *root*. Se ha asignado el identificador CVE-2019-16011 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Actualización de seguridad 5.4.1 para WordPress

Fecha de publicación: 30/04/2020

Importancia: Alta

Recursos afectados:

WordPress, versiones 5.4 y anteriores.

Descripción:

Se ha publicado la última versión de WordPress, que corrige 7 problemas de seguridad.

Solución:

- Actualizar a la versión 5.4.1,
- Todas las versiones de WordPress, desde la 3.7 también tienen disponible la actualización.

Detalle:

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

- visualizar contenidos no publicados sin autenticación,
- fallo en el reinicio de los *tokens* de las contraseñas,
- un ataque del tipo *Cross-site scripting* en *Customizer,*
- un ataque del tipo *Cross-site scripting* en el cuadro de búsquedas,
- un ataque del tipo *Cross-site scripting* en *wp-object-cache,*
- un ataque del tipo *Cross-site scripting* en la subida de archivos,
- un ataque del tipo *Cross-site scripting* almacenado en WordPress *customizer,*
- un ataque del tipo *Cross-site scripting* en el *block editor*.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos F5

Fecha de publicación: 30/04/2020

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:
  - desde 11.6.1 hasta 11.6.5;
  - desde 12.1.0 hasta 12.1.5;
  - desde 13.1.0 hasta 13.1.3;
  - desde 14.0.0 hasta 14.1.2;
  - desde 15.0.0 hasta 15.0.1, y 15.1.0.
- BIG-IQ Centralized Management, versiones:
  - desde 5.3.0 hasta 5.4.0;
  - desde 6.0.0 hasta 6.1.0;
  - desde 7.0.0 hasta 7.1.0.

Descripción:

Se han identificado 8 vulnerabilidades, todas de severidad alta, en varios productos de F5, de tipo: uso de cifrados en servidores de *backend*, fallo en la aceleración criptográfica de *hardware*, envío de solicitud maliciosa por *scp* (*secure copy*), envío de solicitudes específicamente diseñadas a un servidor virtual, generar un archivo de núcleo y reiniciar TMM (*Traffic Management Microkernel*), intentos de conexión sin cifrar a un nuevo *peer* de sincronización, datos de entrada malformados y procesamiento de tráfico IP inusual.

Solución:

Actualizar BIG-IP a alguna de las siguientes versiones:

- 11.6.5.1,
- 12.1.5, 12.1.5.1;
- 13.1.3.2,
- 14.0.1.1, 14.1.2.4;
- 15.0.0, 15.0.1.1, 15.0.1.2, 15.0.1.3, 15.1.0, 15.1.0.2.

Detalle:

Un atacante que aproveche las vulnerabilidades descritas podría realizar las siguientes acciones en los productos afectados:

- denegación de servicio (DoS),
- evento de conmutación por error (*failover event*),
- ejecución de comandos arbitrarios con privilegios elevados,
- interrupción del servicio,
- interrupción del flujo de tráfico, provocando una conmutación por error (*failover*) a un sistema en espera,
- obtener y/o modificar información sensible en el sistema,
- fallo en el procesamiento de tráfico.

Se han reservado los identificadores CVE-2020-5871, CVE-2020-5872, CVE-2020-5873, CVE-2020-5874, CVE-2020-5875, CVE-2020-5876, CVE-2020-5877 y CVE-2020-5878 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad