Boletín de octubre de 2020

Avisos Técnicos

Múltiples vulnerabilidades en HPE IP Console Switch G2 4x1Ex32

Fecha de publicación: 01/10/2020

Importancia: Crítica

Recursos afectados:

HPE KVM IP Console Switches G2 4x1Ex32, versiones anteriores a 2.8.3.

Descripción:

Nikita Medvedev, investigador de Yandex, ha reportado 2 vulnerabilidades, ambas con severidad crítica, de tipo XSS almacenado y ejecución remota de código.

Solución:

Actualizar el producto afectado a la versión 2.8.3.

Detalle:

Las vulnerabilidades podrían ser utilizadas por un atacante remoto para realizar ataques de XSS (*Cross-Site Scripting*) almacenado o ejecuciones de código (RCE). Se han asignado los identificadores CVE-2020-24627 y CVE-2020-24628 para estas vulnerabilidades.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Microsoft Azure Sphere

Fecha de publicación: 07/10/2020

Importancia: Crítica

Recursos afectados:

Microsoft Azure Sphere, versiones 20.06 y 20.07.

Descripción:

Lilith Wyatt, Claudio Bozzato y Dave McDaniel, investigadores de Cisco Talos, han descubierto 4 vulnerabilidades, 2 con severidad crítica, una alta y una media, de tipos denegación de servicio, fuga de información, ejecución de código y corrupción de memoria.

Solución:

Los investigadores de Cisco Talos no han especificado soluciones, aunque siempre se recomienda actualizar los productos a la última versión disponible, actualmente la 20.08.

Detalle:

- Existe una vulnerabilidad de denegación de servicio (DoS) en la funcionalidad *Littlefs Quota* de Microsoft Azure Sphere 20.06. Un conjunto de llamadas especialmente diseñado al sistema podría provocar que se omita la cuota y se reinicie. Un atacante podría realizar llamadas al sistema para activar esta vulnerabilidad.
- Existe una vulnerabilidad de corrupción de memoria en la funcionalidad *SIGN_WITH_TENANT_ATTESTATION_KEY*, perteneciente al controlador del *kernel /dev/pluton*, de Microsoft Azure Sphere 20.07. Una secuencia especialmente diseñada de llamadas *ioctl* podría provocar daños en la memoria en Pluton. Un atacante podría emitir una llamada *ioctl* desde *Normal World* para desencadenar esta vulnerabilidad.

El resto de vulnerabilidades no críticas son de tipo: divulgación de memoria y ejecución de código.

Etiquetas: 0day, IoT, Microsoft, Vulnerabilidad

Múltiples vulnerabilidades en HP Device Manager

Fecha de publicación: 07/10/2020

Importancia: Crítica

Recursos afectados:

Todas las versiones de HP Device Manager.

Descripción:

El investigador de seguridad Nick Bloor ha notificado 3 vulnerabilidades al HP PRST (*Product Security Response Team*), una con severidad crítica y 2 altas, de tipos invocación de método remoto, cifrado débil y elevación de privilegios.

Solución:

- HP Device Manager 4.7: se publicará próximamente *Service Pack* 13 para solucionar estas vulnerabilidades;
- HP Device Manager 5.0: actualizar a la versión 5.0.4.

Detalle:

- Esta vulnerabilidad podría permitir que un atacante remoto obtuviese acceso no autorizado a los recursos. Se ha asignado el identificador CVE-2020-6926 para esta vulnerabilidad crítica.
- Esta vulnerabilidad podría permitir que las cuentas administradas localmente dentro de HP Device Manager fuesen susceptibles a ataques de diccionario debido a una implementación de cifrado débil. No afecta a los clientes que utilizan cuentas autenticadas de Active Directory. Se ha asignado el identificador CVE-2020-6925 para esta vulnerabilidad.
- Esta vulnerabilidad podría permitir que un atacante obtuviese privilegios de *SYSTEM*. No afecta a los clientes que utilizan una base de datos externa (Microsoft SQL Server) y no han instalado el servicio integrado Postgres. Se ha asignado el identificador CVE-2020-6927 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Helpdesk de QNAP

Fecha de publicación: 09/10/2020

Importancia: Crítica

Recursos afectados:

QNAP Helpdesk, versiones anteriores a 3.0.3.

Descripción:

Jose Antonio Pérez Piedra ha reportado 2 vulnerabilidades, de severidad crítica, que afectan a dispositivos de QNAP.

Solución:

Actualizar Helpdesk a la versión 3.0.3 o posteriores, siguiendo las instrucciones del apartado *Updating Helpdesk* del aviso de QNAP.

Detalle:

- Esta vulnerabilidad, de control de acceso inadecuado, podría permitir a los atacantes obtener el control de un dispositivo QNAP. Se ha asignado el identificador CVE-2020-2506 para esta vulnerabilidad.
- Esta vulnerabilidad, de control de acceso inadecuado, podría permitir a los atacantes obtener el control de un dispositivo QNAP. Se ha asignado el identificador CVE-2020-2507 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Privacidad, Vulnerabilidad

---

Múltiples vulnerabilidades de escalada de privilegios en Acronis True Image, Cyber Backup y

Cyber Protection

Fecha de publicación: 13/10/2020

Importancia: Alta

Recursos afectados:

Versiones anteriores a:

- Acronis True Image 2021 build 32010,
- Acronis Cyber ??Backup 12.5 build 16363,
- Acronis Cyber ??Protect 15 build 24600.

Descripción:

Investigadores del CERT/CC, e independientes a través de HackerOne, han informado a Acronis de varias vulnerabilidades de secuestro de búsqueda de DLL, lo que permitiría a un atacante con acceso local al sistema modificar ficheros DLL y de configuración que se cargan al inicio del programa, causando una escalda de privilegios en entornos Windows permitiendo ejecutar código con privilegios SYSTEM.

Solución:

Se recomienda instalar las siguientes versiones para solucionar esas vulnerabilidades:

- Acronis True Image 2021 build 32010,
- Acronis Cyber ??Backup 12.5 build 16363,
- Acronis Cyber ??Protect 15 build 24600.

Detalle:

Se han descubierto tres vulnerabilidades de secuestro de búsqueda de DLL, lo que permitiría a un atacante con acceso local al sistema modificar ficheros DLL y de configuración, causando una escalda de privilegios con privilegios SYSTEM.

- Debido a que los usuarios de Windows sin privilegios pueden crear subdirectorios fuera de la raíz del sistema, un usuario puede crear la ruta adecuada dentro *C:jenkins_agent* para cargar un fichero *openssl.cnf* especialmente modificado para lograr la ejecución de código con privilegios. Esta vulnerabilidad afecta a los 3 productos de Acronis y se han asignado los identificadores CVE-2020-10138 y CVE-2020-10139 para esta vulnerabilidad.
- Debido a que Acronis True Image 2021 no configura correctamente las ACL en la ruta *C:ProgramDataAcronis*, un usuario sin privilegios puede ejecutar código arbitrario con privilegios, colocando una DLL modificada dentro de esa ruta. Se han asignado el identificador CVE-2020-10140 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad, Windows

Boletín de seguridad de Microsoft de octubre de 2020

Fecha de publicación: 14/10/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Microsoft JET Database Engine;
- Azure Functions;
- Open Source Software;
- Microsoft Exchange Server;
- Visual Studio;
- PowerShellGet;
- Microsoft .NET Framework;
- Microsoft Dynamics;
- Adobe Flash Player;
- Microsoft Windows Codecs Library.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de octubre, consta de 83 vulnerabilidades, 11 clasificadas como críticas y 72 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:

- escalada de privilegios,
- ejecución remota de código,
- divulgación de información,

- denegación de servicio,
- elusión de las medidas de seguridad,
- suplantación de identidad (*spoofing*).

Etiquetas: Actualización, Adobe, Comunicaciones, Microsoft, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en productos Juniper

Fecha de publicación: 15/10/2020

Importancia: Crítica

Recursos afectados:

- Junos OS, versiones: 12.3, 12.3X48, 15.1, 15.1X49, 16.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3 y 19.4, 20.1;
- Mist Cloud UI;
- Contrail Networking.

Descripción:

Juniper ha publicado varios avisos de seguridad que recogen múltiples vulnerabilidad, entre las que destacan 3 de severidad crítica, de tipo ejecución arbitraria de código en el servidor Telnet, gestión incorrecta de respuestas en SAML y ejecución arbitraria de código al procesar archivos YAML no confiables.

Solución:

- Actualizar Junos OS a alguna de las siguientes versiones: 12.3R12-S16, 12.3X48-D105, 15.1R7-S7, 15.1X49-D220, 15.1X49-D230, 16.1R7-S8, 17.2R3-S4, 17.2X75-D45, 17.3R3-S8, 17.3R3-S9, 17.4R2-S11, 17.4R3-S2, 18.1R3-S10, 18.2R3-S5, 18.2X75-D34, 18.2X75-D41, 18.2X75-D430, 18.2X75-D65, 18.3R2-S4, 18.3R3-S3, 18.4R2-S5, 18.4R3-S4, 19.1R2-S2, 19.1R3-S2, 19.2R1-S5, 19.2R2, 19.2R2-S1, 19.2R3, 19.3R2-S3, 19.3R3, 19.4R1-S3, 19.4R2-S1, 19.4R3, 20.1R1-S2, 20.1R2, 20.2R1, 20.3X75-D10 y todos los lanzamientos posteriores;
- Mist Cloud UI se actualizó el 2 de septiembre de 2020 para resolver sus vulnerabilidades;
- actualizar Contrail Networking a la versión R2008.

Todas las actualizaciones están disponibles en el centro de descargas de Juniper.

Detalle:

- Una vulnerabilidad en el servidor Telnet *telnetd* permitiría a atacantes remotos ejecutar código arbitrario a través de escrituras cortas o datos urgentes, debido a un desbordamiento del búfer que involucra las funciones *netclear* y *nextitem*. Se ha asignado el identificador CVE-2020-10188 para esta vulnerabilidad.
- Mist Cloud UI, cuando la autenticación SAML está habilitada, puede gestionar incorrectamente las respuestas SAML (*Security Assertion Markup Language*), permitiendo que un atacante remoto eluda los controles de seguridad de autenticación SAML. Se han asignado los identificadores CVE-2020-1675, CVE-2020-1676 y CVE-2020-1677 para estas vulnerabilidades, que pueden explotarse solas o combinadas.
- Una vulnerabilidad en la biblioteca PyYAML podría permitir la ejecución de código arbitrario cuando procesa archivos YAML (*YAML Ain't Markup Language*) que no son de confianza a través del método *full_load* o con el cargador *FullLoader*. Se ha asignado el identificador CVE-2020-1747 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Actualización de seguridad de SAP de octubre de 2020

Fecha de publicación: 15/10/2020

Importancia: Crítica

Recursos afectados:

- SAP Solution Manager y SAP Focused Run, versiones 9.7, 10.1, 10.5 y 10.7;
- SAP Business Client, versión 6.5;
- SAP NetWeaver, versiones 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, 7.51, 7.53 y 7.55;
- SAP Business Objects Business Intelligence Platform, versiones 4.1, 4.2 y 4.3;
- SAP Landscape Management, versión 3.0;
- SAP Adaptive Extensions, versión 1.0;
- SAP 3D Visual Enterprise Viewer, versión 9;
- SAP Commerce Cloud, versiones 1808, 1811, 1905 y 2005;
- SAP Business Planning y Consolidation, versiones 750, 751, 752, 753, 754, 755, 810, 100 y 200;
- SAP ERP (HCM Travel Management); versiones 600, 602, 603, 604, 605, 606, 607 y 608;
- SAP Banking Services, versión 500.

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 15 notas de seguridad y 6 actualizaciones de notas anteriores, siendo 2 de las nuevas notas de severidad crítica, 7 altas, 11 medias y 1 baja.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 6 vulnerabilidades de XSS (*Cross-Site Scripting*),
- 3 vulnerabilidades de divulgación de información,
- 1 vulnerabilidad de control de inyección de código,
- 1 vulnerabilidad de falta de comprobación de autenticación,
- 1 vulnerabilidad de falta de validación de XML,
- 1 vulnerabilidad de credenciales embebidas en claro,
- 1 vulnerabilidad de inyección de comandos en el SSOO,
- 12 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- La vulnerabilidad podría permitir a un atacante inyectar comandos del sistema operativo y así obtener el control completo del host que ejecuta CA Introscope Enterprise Manager. Se ha asignado el identificador CVE-2020-63640 para esta vulnerabilidad.
- Actualización de la nota de seguridad de abril 2018 para el control del navegador Google Chromium entregado con SAP Business Client.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-6296, CVE-2020-6367, CVE-2020-6366, CVE-2020-6369, CVE-2020-6309, CVE-2020-6237, CVE-2020-6236, CVE-2020-6319, CVE-2020-6315, CVE-2020-6372, CVE-2020-6373, CVE-2020-6374, CVE-2020-6375, CVE-2020-6376, CVE-2020-6272, 6368, CVE-2020-6301, CVE-2020-6308, CVE-2020-6370, CVE-2020-6365, CVE-2020-6323, CVE-2020-6371, CVE-2020-6362 y CVE-2020-6363.

Etiquetas: Actualización, SAP, Vulnerabilidad

Ejecución remota de código en Visual Studio y Microsoft Windows Codecs Library

Fecha de publicación: 19/10/2020

Importancia: Alta

Recursos afectados:

- Windows 10 versión 1709 para sistemas de 32 bit,
- Windows 10 versión 1709 para sistemas basados en ARM64,
- Windows 10 versión 1709 para sistemas basados en x64,
- Windows 10 versión 1803 para sistemas de 32 bit,
- Windows 10 versión 1803 para sistemas basados en ARM64,
- Windows 10 versión 1803 para sistemas basados en x64,
- Windows 10 versión 1809 para sistemas de 32 bit,
- Windows 10 versión 1809 para sistemas basados en ARM64,
- Windows 10 versión 1809 para sistemas basados en x64,
- Windows 10 versión 1903 para sistemas de 32 bit,
- Windows 10 versión 1903 para sistemas basados en ARM64,
- Windows 10 versión 1903 para sistemas basados en x64,
- Windows 10 versión 1909 para sistemas basados en ARM64,
- Windows 10 versión 1909 para sistemas basados en x64,
- Windows 10 versión 2004 para sistemas de 32 bit,
- Windows 10 versión 2004 para sistemas basados en ARM64,
- Windows 10 versión 2004 para sistemas basados en x64,
- Visual Studio Code.

Descripción:

Microsoft ha publicado dos avisos de seguridad para corregir las vulnerabilidades de ejecución remota de código en los productos afectados.

Solución:

- Para Windows Media Codec la actualización corrige la forma en que Microsoft Windows Codecs Library maneja los objetos en memoria, los clientes afectados se actualizarán automáticamente desde Microsoft Store.
- Para Visual Studio, descargar la última versión que modifica la forma en que el código de Visual Studio maneja los archivos JSON.

Detalle:

- Una vulnerabilidad en la biblioteca de códecs de Microsoft Windows, al manejar los objetos en la memoria, podría permitir a un atacante la ejecución remota de código mediante el procesado de un archivo de imagen especialmente diseñado. Se ha asignado el identificador CVE-2020-17022 para esta vulnerabilidad.
- Una vulnerabilidad presente en el código de Visual Studio podría permitir a un atacante ejecutar código arbitrario en el contexto del usuario actual, si logra engañar a ese usuario para que clone un repositorio y abra un archivo 'package.json' malicioso. Se ha asignado el identificador CVE-2020-17023 para esta vulnerabilidad.

Etiquetas: Actualización, Microsoft, Vulnerabilidad, Windows

Desbordamiento de búfer basado en pila en SonicOS de SonicWall

Fecha de publicación: 20/10/2020

Importancia: Crítica

Recursos afectados:

SonicOS, versiones:

- 6.5.4.6-79n y anteriores;
- 6.5.1.11-4n y anteriores;
- 6.0.5.3-93o y anteriores;
- 6.5.4.4-44v-21-794 y anteriores;
- 7.0.0.0-1.

Descripción:

Los investigadores, Nikita Abramov, de Positive Technologies, y Craig Young, de Tripwire, han descubierto una vulnerabilidad, de severidad crítica, que afecta a varias versiones de SonicOS, el sistema operativo de SonicWall.

Solución:

- Actualizar SonicOS a alguna de las siguientes versiones:
  - 6.5.4.7-83n;
  - 6.5.1.12-1n;
  - 6.0.5.3-94o;
  - 6.5.4.v-21s-987;
  - 7 7.0.0.0-2 o posteriores.

Detalle:

Una vulnerabilidad de desbordamiento de búfer basado en pila (*stack*) en SonicOS podría permitir que un atacante remoto, no autenticado, provocase una condición de denegación de servicio (DoS) y ejecutase código arbitrario enviando una solicitud maliciosa al *firewall*. Se ha asignado el identificador CVE-2020-5135 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Privacidad, Vulnerabilidad

---

Actualizaciones críticas en Oracle (octubre 2020)

Fecha de publicación: 21/10/2020

Importancia: Crítica

Recursos afectados:

- Application Performance Management (APM), versiones 13.3.0.0, 13.4.0.0;
- Big Data Spatial and Graph, versiones anteriores a 3.0;
- Enterprise Manager Base Platform, versiones 13.2.1.0, 13.3.0.0, 13.4.0.0;
- Enterprise Manager for Peoplesoft, versión 13.4.1.1;
- Enterprise Manager for Storage Management, versiones 13.3.0.0, 13.4.0.0;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versiones anteriores a XCP2362, y anteriores a XCP3090;
- Fujitsu M12-1, M12-2, M12-2S Servers, versiones anteriores a XCP3090;
- Hyperion Analytic Provider Services, versión 11.1.2.4;
- Hyperion BI , versión 11.1.2.4;
- Hyperion Essbase, versión 11.1.2.4;
- Hyperion Infrastructure Technology, versión 11.1.2.4;
- Hyperion Lifecycle Management, versión 11.1.2.4;
- Hyperion Planning, versión 11.1.2.4;
- Identity Manager Connector, versión 9.0;
- Instantis EnterpriseTrack, versiones 17.1, 17.2, 17.3;
- Management Pack for Oracle GoldenGate, versión 12.2.1.2.0;
- MySQL Cluster, versiones 7.3.30 y anteriores, 7.4.29 y anteriores, 7.5.19 y anteriores, 7.6.15 y anteriores, 8.0.21 y anteriores;
- MySQL Enterprise Monitor, versiones 8.0.21 y anteriores;
- MySQL Server, versiones 5.6.49 y anteriores, 5.7.31 y anteriores, 8.0.21 y anteriores;
- MySQL Workbench, versiones 8.0.21 y anteriores;
- Oracle Access Manager, versión 11.1.2.3.0;
- Oracle Agile PLM, versiones 9.3.3, 9.3.5, 9.3.6;
- Oracle Agile Product Lifecycle Management for Process, versión 6.2.0.0;
- Oracle Application Express, versiones anteriores a 20.2;
- Oracle Application Testing Suite, versión 13.3.0.1;
- Oracle Banking Corporate Lending, versiones 12.3.0, 14.0.0-14.4.0;
- Oracle Banking Digital Experience, versiones 18.1, 18.2, 18.3, 19.1, 19.2, 20.1;
- Oracle Banking Payments, versiones 14.1.0-14.4.0;
- Oracle Banking Platform, versiones 2.4.0-2.10.0;
- Oracle BI Publisher, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle Business Process Management Suite, versiones 12.2.1.3.0, 12.2.1.4.0;

- Oracle Communications Application Session Controller, versiones 3.8m0, 3.9m0p1;
- Oracle Communications Billing and Revenue Management, versiones 7.5.0.23.0, 12.0.0.2.0, 12.0.0.3.0;
- Oracle Communications BRM - Elastic Charging Engine, versiones 11.3.0.9.0, 12.0.0.3.0;
- Oracle Communications Diameter Signaling Router (DSR), versiones 8.0.0.0-8.4.0.5, [IDIH] 8.0.0-8.2.2;
- Oracle Communications EAGLE Software, versiones 46.6.0-46.8.2;
- Oracle Communications Element Manager, versiones 8.2.0-8.2.2;
- Oracle Communications Evolved Communications Application Server, versión 7.1;
- Oracle Communications Messaging Server, versión 8.1;
- Oracle Communications Offline Mediation Controller, versión 12.0.0.3.0;
- Oracle Communications Services Gatekeeper, versión 7;
- Oracle Communications Session Border Controller, versiones 8.2-8.4;
- Oracle Communications Session Report Manager, versiones 8.2.0-8.2.2;
- Oracle Communications Session Route Manager, versiones 8.2.0-8.2.2;
- Oracle Communications Unified Inventory Management, versiones 7.3.0, 7.4.0;
- Oracle Communications WebRTC Session Controller, versión 7.2;
- Oracle Data Integrator, versiones 11.1.1.9.0, 12.2.1.3.0;
- 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, 12.2.3-12.2.10;
- Oracle Endeca Information Discovery Integrator, versión 3.2.0;
- Oracle Endeca Information Discovery Studio, versión 3.2.0;
- Oracle Enterprise Repository, versión 11.1.1.7.0;
- Oracle Enterprise Session Border Controller, versión 8.4;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 8.0.6-8.1.0;
- Oracle Financial Services Analytical Applications Reconciliation Framework, versiones 8.0.6-8.0.8, 8.1.0;
- Oracle Financial Services Asset Liability Management, versiones 8.0.6, 8.0.7, 8.1.0;
- Oracle Financial Services Balance Sheet Planning, versión 8.0.8;
- Oracle Financial Services Basel Regulatory Capital Basic, versiones 8.0.6-8.0.8, 8.1.0;
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versiones 8.0.6-8.0.8, 8.1.0;
- Oracle Financial Services Data Foundation, versiones 8.0.6-8.1.0;
- Oracle Financial Services Data Governance for US Regulatory Reporting, versiones 8.0.6-8.0.9;
- Oracle Financial Services Data Integration Hub, versiones 8.0.6, 8.0.7, 8.1.0;
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.6, 8.0.7, 8.1.0;
- Oracle Financial Services Hedge Management and IFRS Valuations, versiones 8.0.6-8.0.8, 8.1.0;
- Oracle Financial Services Institutional Performance Analytics, versiones 8.0.6, 8.0.7, 8.1.0, 8.7.0;
- 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, 8.1.0;
- Oracle Financial Services Loan Loss Forecasting and Provisioning, versiones 8.0.6-8.0.8, 8.1.0;
- Oracle Financial Services Market Risk Measurement and Management, versiones 8.0.6, 8.0.8, 8.1.0;
- Oracle Financial Services Price Creation and Discovery, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Profitability Management, versiones 8.0.6, 8.0.7, 8.1.0;
- Oracle Financial Services Regulatory Reporting for European Banking Authority, versiones 8.0.6-8.1.0;
- Oracle Financial Services Regulatory Reporting for US Federal Reserve, versiones 8.0.6-8.0.9;
- Oracle Financial Services Regulatory Reporting with AgileREPORTER, versión 8.0.9.2.0;
- Oracle Financial Services Retail Customer Analytics, versión 8.0.6;
- Oracle FLEXCUBE Core Banking, versiones 5.2.0, 11.5.0-11.7.0;
- Oracle FLEXCUBE Direct Banking, versiones 12.0.1, 12.0.2, 12.0.3;
- Oracle FLEXCUBE Private Banking, versiones 12.0.0, 12.1.0;
- Oracle FLEXCUBE Universal Banking, versiones 12.3.0, 14.0.0-14.4.0;
- Oracle GoldenGate Application Adapters, versiones 12.3.2.1.0, 19.1.0.0.0;
- Oracle GraalVM Enterprise Edition, versiones 19.3.3, 20.2.0;
- Oracle Health Sciences Empirica Signal, versión 9.0;
- Oracle Healthcare Data Repository, versión 7.0.1;
- Oracle Healthcare Foundation, versiones 7.1.1, 7.2.0, 7.2.1, 7.3.0;
- Oracle Hospitality Guest Access, versiones 4.2.0, 4.2.1;
- Oracle Hospitality Materials Control, versión 18.1;
- Oracle Hospitality OPERA 5 Property Services, versiones 5.5, 5.6;
- Oracle Hospitality Reporting and Analytics, versión 9.1.0;
- Oracle Hospitality RES 3700, versión 5.7;
- Oracle Hospitality Simphony, versiones 18.1, 18.2, 19.1.0-19.1.2;
- Oracle Hospitality Suite8, versiones 8.10.2, 8.11-8.15;
- Oracle HTTP Server, versiones 12.2.1.3.0, 12.2.1.4.0;
- Oracle Insurance Accounting Analyzer, versión 8.0.9;
- Oracle Insurance Allocation Manager for Enterprise Profitability, versiones 8.0.8, 8.1.0;
- Oracle Insurance Data Foundation, versiones 8.0.6-8.1.0;
- Oracle Insurance Insbridge Rating and Underwriting, versiones 5.0.0.0-5.6.0.0, 5.6.1.0;
- Oracle Insurance Policy Administration J2EE, versiones 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26, 11.2.2.0;
- Oracle Insurance Rules Palette, versiones 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26;
- Oracle Java SE, versiones 7u271, 8u261, 11.0.8, 15;
- Oracle Java SE Embedded, versión 8u261;
- Oracle JDeveloper, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- 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 Policy Automation, versiones 12.2.0-12.2.20;
- Oracle Policy Automation Connector for Siebel, versión 10.4.6;
- Oracle Policy Automation for Mobile Devices, versiones 12.2.0-12.2.20;
- Oracle REST Data Services, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c, [Standalone ORDS] y anteriores a 20.2.1;
- Oracle Retail Advanced Inventory Planning, versión 14.1;
- Oracle Retail Assortment Planning, versiones 15.0.3.0, 16.0.3.0;
- Oracle Retail Back Office, versiones 14.0, 14.1;
- Oracle Retail Bulk Data Integration, versiones 15.0.3.0, 16.0.3.0;
- Oracle Retail Central Office, versiones 14.0, 14.1;
- Oracle Retail Customer Management and Segmentation Foundation, versiones 18.0, 19.0;
- Oracle Retail Integration Bus, versiones 14.1, 15.0, 16.0;
- Oracle Retail Order Broker, versiones 15.0, 16.0, 18.0, 19.0, 19.1, 19.2, 19.3;
- Oracle Retail Point-of-Service, versiones 14.0, 14.1;
- Oracle Retail Predictive Application Server, versiones 14.1.3.0, 15.0.3.0, 16.0.3.0;
- Oracle Retail Price Management, versiones 14.0.4, 14.1.3.0, 15.0.3.0, 16.0.3.0;

- Oracle Retail Returns Management, versiones 14.0, 14.1;
- Oracle Retail Service Backbone, versiones 14.1, 15.0, 16.0;
- Oracle Retail Xstore Point of Service, versiones 15.0.3, 16.0.5, 17.0.3, 18.0.2, 19.0.1;
- Oracle Solaris, versiones 10, 11;
- Oracle TimesTen In-Memory Database, versiones anteriores a 11.2.2.8.49, 18.1.3.1.0, y anteriores a 18.1.4.1.0;
- Oracle Transportation Management, versión 6.3.7;
- Oracle Utilities Framework, versiones 2.2.0.0.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0;
- Oracle VM VirtualBox, versiones anteriores a 6.1.16;
- Oracle WebCenter Portal, versiones 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0;
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0;
- Oracle ZFS Storage Appliance Kit, versión 8.8;
- PeopleSoft Enterprise HCM Global Payroll Core, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57, 8.58;
- PeopleSoft Enterprise SCM eSupplier Connection, versión 9.2;
- Primavera Gateway, versiones 16.2.0-16.2.11, 17.12.0-17.12.8;
- Primavera Unifier, versiones 16.1, 16.2, 17.7-17.12, 18.8, 19.12;
- Siebel Applications, versiones 20.7, 20.8.

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

Etiquetas: Actualización, Java, Oracle, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 21/10/2020

Importancia: Crítica

Recursos afectados:

- ESXi, versiones 6.7 y 6.5;
- Workstation Pro / Player (Workstation), versión 15.x;
- Fusion Pro / Fusion (Fusion), versión 11.x (ejecutándose en OS X);
- NSX-T, versiones 3.x y 2.5.x;
- Cloud Foundation, versiones 4.x (para las vulnerabilidades CVE-2020-3992, CVE-2020-3993, CVE-2020-3981 yCVE-2020-3982) y 3.x;
- vCenter Server, versiones 6.7 (ejecutándose en Virtual Appliance) y 6.5 (ejecutándose en Virtual Appliance).

Descripción:

Diversos investigadores han reportado a VMware 6 vulnerabilidades, 1 de severidad crítica, 4 altas y 1 media, de tipos uso de la memoria previamente liberada, MitM (*man in the middle*), lectura fuera de límites, secuestro de sesión (*hijacking*), pérdida de memoria y escritura fuera de límites.

Solución:

Se recomienda instalar los últimos parches para los productos afectados, en función de la versión estable utilizada, indicados en la columna *Fixed Version* de cada tabla *Response Matrix* correspondiente.

Detalle:

La vulnerabilidad con severidad crítica permitiría que un atacante, con acceso a la red de administración y al puerto 427 en una máquina ESXi, pudiese realizar una ejecución remota de código al aprovechar la vulnerabilidad de memoria previamente liberada en el servicio OpenSLP. Se ha asignado el identificador CVE-2020-3992 para esta vulnerabilidad.

Otros identificadores asignados para el resto de vulnerabilidades son CVE-2020-3981, CVE-2020-3982, CVE-2020-3993, CVE-2020-3994 y CVE-2020-3995.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad

---

Vulnerabilidad de divulgación de información privilegiada en varios productos de HPE

Fecha de publicación: 22/10/2020

Importancia: Crítica

Recursos afectados:

- BlueData EPIC Software, versión 4.0 y anteriores;
- HPE Ezmeral Container Platform, versión 5.0.

Descripción:

Hamoon Raphael Mehran, de Early Warning Security, ha reportado una vulnerabilidad, de severidad crítica, de tipo divulgación remota de información privilegiada.

Solución:

- La versión 4.0 de BlueData EPIC Software Platform dispone de un parche que soluciona la vulnerabilidad. Contactar con el soporte técnico de HPE para obtenerlo;
- actualizar HPE Ezmeral Container Platform a la versión 5.1 o posteriores.

Detalle:

Los productos afectados por esta vulnerabilidad utilizan un método inseguro en la gestión de contraseñas de Kerberos, que es susceptible a que las contraseñas sean interceptadas y/o recuperadas sin autorización. Concretamente, se muestra *kdc_admin_password* en el archivo fuente de la URL */bdswebui/assignusers/*. Se ha asignado el identificador CVE-2020-7196 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Escalada de privilegios en Chocolatey Boxstarter

Fecha de publicación: 23/10/2020

Importancia: Alta

Recursos afectados:

Chocolatey Boxstarter, versión 2.12.0 y anteriores.

Descripción:

Will Dormann ha reportado al CERT/CC una vulnerabilidad, de severidad alta, que podría permitir a un atacante la escalada de privilegios en Chocolatey Boxstarter.

Solución:

Actualizar a la versión 2.13.0.

Detalle:

El instalador de Chocolatey Boxstarter falla al establecer una lista de control de acceso seguro (ACL) en el directorio *C:ProgramDataBoxstarter*, que se añade a la variable de entorno *PATH* del sistema. La vulnerabilidad podría permitir a un atacante la escalada de privilegios, ya que cualquier ubicación en la variable de entorno *PATH* de todo el sistema, puede utilizarse para cargar código que se ejecuta con privilegios. Se ha asignado el identificador CVE-2020-15264 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Omisión de autenticación remota en HPE SSMC

Fecha de publicación: 26/10/2020

Importancia: Crítica

Recursos afectados:

HPE 3PAR StoreServ Management y Core Software Media, versiones anteriores a 3.7.0.0.

Descripción:

Elwood Buck, de MindPoint Group, ha reportado a HPE una vulnerabilidad, de severidad crítica, de tipo omisión de autenticación remota, que afecta al producto StoreServ Management Console (SSMC).

Solución:

- Actualizar HPE 3PAR StoreServ Management Console a la versión 3.7.1.1 o posteriores;
- actualizar SSMC a la versión 3.7.1.1, disponible en *mylicense portal*.

Detalle:

HPE StoreServ Management Console (SSMC), que es una aplicación web de administrador multiarray fuera del nodo y permanece aislada de los datos en las matrices administradas, es vulnerable a la omisión de autenticación remota. Se ha asignado el identificador CVE-2020-7197 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en AirWave Glass de Aruba

Fecha de publicación: 26/10/2020

Importancia: Crítica

Recursos afectados:

AirWave Glass, versión 1.3.1 y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades en AirWave Glass de Aruba que podrían permitir a un atacante la ejecución remota de código, comprometer totalmente el sistema, escalar privilegios o realizar ataques Server Side Request Forgery.

Solución:

Actualizar a Airwave Glass versión 1.3.2 o superior.

Detalle:

- La exposición de los servicios de gestión de contenedores de manera no autenticada podrían permitir a un atacante la ejecución remota de código. Se han asignado los identificadores CVE-2020-7127 y CVE-2020-7128 para estas vulnerabilidades.
- Los atacantes con acceso a la interfaz de gestión de la web podrían aprovechar una vulnerabilidad que permite acceder al sistema de gestión del contenedor para lograr un compromiso completo del sistema anfitrión. Se ha asignado el identificador CVE-2020-7124 para esta vulnerabilidad.
- La validación inadecuada del control de acceso podría permitir a un usuario, con privilegios de sólo lectura, la escalada de privilegios al añadir nuevos usuarios o alterar las propiedades de los usuarios con más privilegios. Se ha asignado el identificador CVE-2020-7125 para esta vulnerabilidad.
- Un usuario con privilegios de glassadmin podría ejecutar código arbitrario como *root* en el sistema operativo del host subyacente a través de *cristaladmin cli*. Se han asignado los identificadores CVE-2020-7129, CVE-2020-24631 y CVE-2020-24632 para estas vulnerabilidades.
- Airwave Glass expone un *endpoint* no autenticado en el subsistema Grafana que puede ser utilizado para crear un ataque *Server Side Request Forgery*. Esto podría permitir el filtrado de datos de los *endpoints* del sistema interno. Se ha asignado el identificador CVE-2020-7126 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de escalada de privilegios en Macrium Reflect

Fecha de publicación: 27/10/2020

Importancia: Alta

Recursos afectados:

Macrium Reflect, versiones anteriores a 7.3.5281.

Descripción:

Will Dormann, del CERT/CC, ha reportado una vulnerabilidad, de severidad alta, de tipo escalada de privilegios, originada por el uso de una variable *OPENSSLDIR* que especifica una ubicación donde un usuario de Windows sin privilegios puede crear archivos.

Solución:

Actualizar Macrium Reflect a la versión 7.3.5281.

Detalle:

Un componente OpenSSL vulnerable, incluido en Macrium Reflect, podría permitir a un atacante, sin privilegios, realizar una ejecución de código arbitrario con privilegios de *SYSTEM* mediante la colocación de un archivo *openssl.cnf* especialmente diseñado en el directorio *C:openssl*. Se ha asignado el identificador CVE-2020-10143 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad, Windows

Múltiples vulnerabilidades en Synology Router Manager

Fecha de publicación: 30/10/2020

Importancia: Crítica

Recursos afectados:

- Synology SRM, versiones:
  - 1.2.3 MR2200ac 8017 y 1.2.3 RT2600ac 8017;
  - 6.2.3 25426 DS120j;
  - 1.2.3 RT2600ac 8017-5.
- Synology QuickConnect.

Descripción:

Cisco Talos ha descubierto recientemente múltiples vulnerabilidades en el software de los router Synology, en Synology Router Manager (SRM) y en QuickConnect. Un atacante remoto podría utilizar estas vulnerabilidades para llevar a cabo una serie de acciones maliciosas, como la ejecución remota de código, la exposición de información sensible relativa a la red de la víctima y la comunicación con otros dispositivos conectados a la misma red.

Solución:

Las reglas de Snort: 53755, 53756, 53839, 53840, 53959 y 54009, pueden utilizarse para detectar los intentos de explotación de estas vulnerabilidades.

Detalle:

La vulnerabilidad, de severidad crítica, en la funcionalidad de servicio lbd de Qualcomm lbd 1.1, presente en Synology SRM 1.2.3 RT2600ac 8017-5, podría permitir a un atacante sobreescribir los archivos de forma arbitraria mediante un comando de depuración especialmente diseñado, resultando en la ejecución remota de código. Se ha asignado el identificador CVE-2020-27654 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2019-11823, CVE-2020-27649, CVE-2020-27651, CVE-2020-27653, CVE-2020-27654, CVE-2020-27655, CVE-2020-27657 y CVE-2020-27658.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Actualización de seguridad 5.5.2 para WordPress

Fecha de publicación: 30/10/2020

Importancia: Alta

Recursos afectados:

WordPress, versiones 5.5.1 y anteriores.

Descripción:

Se ha publicado la última versión de WordPress, que corrige 10 problemas de seguridad.

Solución:

Actualizar a la versión 5.5.2.

Detalle:

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

- inserción de spam,
- realizar XSS (Cross-Site Scripting),
- escalada de privilegios a través XML-RPC,
- ejecución de RCE (Remote Command Execution),
- eliminación arbitraria de archivos,
- realizar CSRF (Cross-Site Request Forgery).

Etiquetas: Actualización, CMS, Vulnerabilidad