Boletín de diciembre de 2020

Avisos Técnicos

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 01/12/2020

Importancia: Crítica

Recursos afectados:

- HP-UX Perl Software E.5.28.0.A;
- HPE Edgeline Infrastructure Management Software, versiones anteriores a la 1.21.

Descripción:

Varias vulnerabilidades, de severidad crítica, podrían permitir a un atacante causar desbordamientos de búfer o ejecutar código arbitrario.

Solución:

Actualizar a:

- Perl E.5.28.0.B;
- HPE Edgeline Infrastructure Manager, versión 1.21 o superior.

Detalle:

- Múltiples vulnerabilidades podrían permitir a un atacante realizar desbordamientos de búfer mediante el uso de expresiones regulares especialmente diseñadas, operaciones de escritura inválidas, inyecciones de intrusión de bytecodes malformados o desbordamientos del búfer en la región heap de la memoria. Se han asignado los identificadores CVE-2018-18311, CVE-2018-18312, CVE-2020-10543, CVE-2020-10878 y CVE-2020-12723 para estas vulnerabilidades.
- La vulnerabilidad de HPE Edgeline Infrastructure Manager, también conocido como HPE Edgeline Infrastructure Management Software, podría ser explotada remotamente para evitar la autenticación remota, lo que podría permitir a un atacante la ejecución de comandos arbitrarios para obtener el acceso privilegiado, causar la denegación de servicio o cambiar la configuración. Se ha asignado el identificador CVE-2020-7199 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en HPE

Fecha de publicación: 02/12/2020

Importancia: Crítica

Recursos afectados:

HP-UX Web Server Suite Software ? HP-UX Apache-based Web Server, versiones 2.4.18.05 y anteriores.

Descripción:

Hewlett Packard Enterprise ha identificado 2 vulnerabilidades de severidad crítica, 8 vulnerabilidades de severidad alta y 5 vulnerabilidades de severidad media. Todas ellas de ejecución remota, y siendo las de severidad crítica aquellas que podrían permitir a un atacante causar divulgación de información sensible y ejecución de código.

Solución:

Actualizar:

- HP-UX Web Server Suite, a la versión 5.10;
- HP-UX Apache-based Web Server, a la version 2.4.43.01.

Detalle:

Dos vulnerabilidades críticas en HPE HP-UX Web Server Suite que ejecuta Apache en HP-UX 11iv3 podrían permitir a un atacante ejecutar código de forma remota o divulgar datos sensibles. Se han asignado los identificadores CVE-2019-10082 y CVE-2020-11984 para estas vulnerabilidades.

Para las vulnerabilidades de severidad alta se han asignado los identificadores CVE-2018-8011, CVE-2019-0190, CVE-2019-0215, CVE-2019-10081, CVE-2019-10097, CVE-2019-9517, CVE-2020-11993 y CVE-2020-9490.

Para las vulnerabilidades de severidad media se han asignado los identificadores CVE-2019-10092, CVE-2019-10098, CVE-2020-11985, CVE-2020-1927 y CVE-2020-1934.

Etiquetas: Actualización, Apache, HP, Vulnerabilidad

Múltiples vulnerabilidades en HP-UX Web Server Suite Software PHP de HPE

Fecha de publicación: 04/12/2020

Importancia: Crítica

Recursos afectados:

HP-UX Web Server Suite Software PHP, versión 7.2.1.1.

Descripción:

Hewlett Packard Enterprise y HPE Product Security Response Team han identificado un total de 13 vulnerabilidades, 2 de severidad crítica, 5 altas y 6 medias, que permitirían a un atacante, local o remoto, omitir restricciones de seguridad, divulgar información y corromper la memoria.

Solución:

Actualizar el producto afectado a la versión PHP 7.4.7.1 para HP-UX Release B.11.31.

Detalle:

- Cuando se utiliza la función *fgetss()* para leer datos con limpieza de etiquetas (*stripping tags*), en varias versiones de PHP sería posible suministrar datos que harían que esta función leyese más allá del búfer asignado. Esto podría llevar a la revelación de información o a un bloqueo. Se ha asignado el identificador CVE-2020-7059 para esta vulnerabilidad crítica.
- Cuando se utilizan ciertas funciones *mbstring* para convertir codificaciones multibyte, en varias versiones de PHP sería posible suministrar datos que harían que la función *mbfl_filt_conv_big5_wchar* leyese más allá del búfer asignado. Esto podría llevar a la divulgación de la información o a un bloqueo. Se ha asignado el identificador CVE-2020-7060 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-7067, CVE-2019-11048, CVE-2020-7066, CVE-2020-7064, CVE-2019-11046, CVE-2019-11044, CVE-2019-11045, CVE-2019-11050, CVE-2019-11047, CVE-2019-11042 y CVE-2019-11041.

Etiquetas: Actualización, HP, PHP, Vulnerabilidad

Actualizaciones de seguridad de Microsoft de diciembre de 2020

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge para Android;
- ChakraCore;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Microsoft Exchange Server;
- Azure DevOps;
- Microsoft Dynamics;
- Visual Studio;
- Azure SDK;
- Azure Sphere.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de diciembre, consta de 58 vulnerabilidades y 1 aviso (ADV200013), 9 clasificadas como críticas, 48 como importantes y 2 moderadas.

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,
- divulgación de información,
- ejecución remota de código,
- elusión de las medidas de seguridad,
- suplantación de identidad (*spoofing*).

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

---

Actualización de seguridad de SAP de diciembre de 2020

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

- SAP NetWeaver AS JAVA, versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver AS ABAP, versiones 620, 640, 700, 710, 730, 731, 740, 750, 751, 752, 753 y 754;
- SAP BusinessObjects BI Platform (Crystal Report), versiones 4.1, 4.2 y 4.3;
- SAP Business Warehouse, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755 y 782;
- SAP BW4HANA, versiones 100 y 200;
- SAP S4 HANA, versiones 101, 102, 103, 104 y 105;
- SAP Solution Manager, versión 7.20;
- SAP Disclosure Management, versión 10.1;
- SAP UI, versiones 7.5, 7.51, 7.52, 7.53 y 7.54;
- SAP UI 700, versión 2.0;
- SAP HANA Database, versión 2.0.

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 11 notas de seguridad y 2 actualizaciones de notas anteriores, siendo 3 de las nuevas notas de severidad crítica, 2 altas, 5 medias y 1 baja.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 2 vulnerabilidades de inyección de código,
- 2 vulnerabilidades de falta de comprobación de autorización,
- 1 vulnerabilidad de *Cross-Site Scripting* (XSS),
- 1 vulnerabilidad de limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*),
- 1 vulnerabilidad de falta de autorización,
- 1 vulnerabilidad de falta de validación de XML,
- 6 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Esta vulnerabilidad podría permitir a un atacante, no autenticado, que fuese capaz de conectarse a los respectivos puertos TCP, realizar diferentes acciones privilegiadas, tales como instalar nuevos proveedores de SSO de confianza, cambiar los parámetros de conexión de la base de datos y obtener acceso a la información de configuración. Se ha asignado el identificador CVE-2020-26829 para esta vulnerabilidad.
- Esta vulnerabilidad podría permitir a un atacante, con privilegios básicos, inyectar entidades XML arbitrarias que llevarían a la divulgación de archivos y directorios internos, y permitirían ataques SSRF y DoS. Se ha asignado el identificador CVE-2020-26831 para esta vulnerabilidad.
- Un atacante, con privilegios elevados, podría enviar peticiones, especialmente elaboradas, para generar y ejecutar código arbitrario sin ninguna interacción adicional del usuario y, por lo tanto, conllevando un potencial compromiso total de la confidencialidad, integridad y disponibilidad del sistema. Se ha asignado el identificador CVE-2020-26838 para esta vulnerabilidad.
- La vulnerabilidad podría permitir que un atacante remoto inyectase y ejecutase un código arbitrario y, de esta manera, tomase el control completo del sistema afectado. Se ha asignado el identificador CVE-2020-26808 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-26837, CVE-2020-26830, CVE-2020-26832, CVE-2020-26826, CVE-2020-26828, CVE-2020-26816, CVE-2020-26835, CVE-2019-0388, CVE-2020-26834 y CVE-2020-26836.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en ArubaOS

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

Las versiones afectadas son:

- ArubaOS: 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0, y anteriores.
- SD-WAN: 2.1.0.1, 2.2.0.0, y anteriores.

Estas versiones se utilizan en los siguientes productos:

- ArubaOS Mobility Conductor.
- Aruba Mobility Controllers.
- Access-Points gestionados por Mobility Controllers.
- Aruba SD-WAN Gateways.

Descripción:

Aruba ha publicado parches para ArubaOS que abordan múltiples vulnerabilidades de seguridad, siendo 2 de ellas críticas y permitiendo a un atacante la ejecución de código remoto no autenticado o la inyección remota de comandos arbitrarios.

Solución:

Se recomienda actualizar ArubaOS a las siguientes versiones:

- ArubaOS 6.4.4.24, 6.5.4.18, 8.2.2.10, 8.3.0.14, 8.5.0.11, 8.6.0.6, 8.7.1.0, y siguientes.
- SD-WAN 2.1.0.2, 2.2.0.1, y siguientes.

Detalle:

Las vulnerabilidades corregidas por Aruba solucionan las siguientes vulnerabilidades críticas:

- Vulnerabilidad de desbordamiento de la memoria intermedia, que podría dar lugar a la ejecución de código remoto no autenticado mediante el envío de paquetes especialmente elaborados destinados al puerto UDP (8211) utilizado por PAPI (Aruba Networks AP management protocol). Se ha asignado el identificador CVE-2020-24633 para esta vulnerabilidad.
- Vulnerabilidad de inyección remota de comandos arbitrarios enviando paquetes especialmente elaborados destinados al puerto UDP (8211) utilizado por PAPI (Aruba Networks AP management protocol). Se ha asignado el identificador CVE-2020-24634 para esta vulnerabilidad.

Se han publicado también parches para vulnerabilidades con los siguientes identificadores asignados: CVE-2020-10713 y CVE-2020-24637.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de credenciales embebidas en IBM Spectrum Protect Plus

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

IBM Spectrum Protect Plus, versiones desde la 10.1.0 hasta la 10.1.6.

Descripción:

Tenable ha identificado una vulnerabilidad, de severidad crítica, de tipo credenciales embebidas.

Solución:

Actualizar a la versión 10.1.7.

Detalle:

El producto afectado contiene credenciales codificadas de forma estática que utiliza para su propia autenticación de entrada, comunicaciones de salida y cifrado de datos internos, lo que podría permitir a un atacante obtener privilegios elevados de forma remota. Se ha asignado el identificador CVE-2020-4854 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de tipo ejecución remota de código en Apache Struts

Fecha de publicación: 09/12/2020

Importancia: Alta

Recursos afectados:

Struts, versiones desde la 2.0.0 hasta la 2.5.25.

Descripción:

Los investigadores, Álvaro Muñoz de GitHub y Masato Anzai de Aeye Security Lab, han informado de una vulnerabilidad, de severidad alta, de tipo ejecución remota de código.

Solución:

Evitar usar la evaluación OGNL (Object Graph Navigation Language) forzada y actualizar a la versión 2.5.26 o superior.

Detalle:

La evaluación forzada de OGNL de los valores de entrada de un usuario que no es de confianza podría provocar una ejecución remota de código (RCE). Se ha asignado el identificador CVE-2020-17530 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Java, Vulnerabilidad

Múltiples vulnerabilidades en Cisco Jabber

Fecha de publicación: 11/12/2020

Importancia: Crítica

Recursos afectados:

- Cisco Jabber para Windows, versiones:
  - anteriores a 12.1;
  - 12.1;
  - 12.5;
  - 12.6;
  - 12.7;
  - 12.8;
  - 12.9.
- Cisco Jabber para MacOS, versiones:
  - 12.7 y anteriores;
  - 12.8;
  - 12.9.
- Cisco Jabber para Android e iOS, versiones:
  - 12.8 y anteriores;
  - 12.9.

Descripción:

Olav Sortland Thoresen, investigador de Watchcom, junto a un equipo de Cisco, que llevó a cabo unas pruebas de seguridad, han detectado 5 vulnerabilidades, 1 de severidad crítica, 2 altas y 2 medias, de tipo inserción de información sensible en los datos enviados, inyección de comandos, inyección de comandos del sistema operativo, divulgación de información y ejecución arbitraria de código.

Solución:

- Cisco Jabber para Windows, versiones:
  - 12.1.4;
  - 12.5.3
  - 12.6.4;
  - 12.7.3;
  - 12.8.4;
  - 12.9.3.
- Cisco Jabber para MacOS, versiones:
  - 12.8.5;
  - 12.9.4.
- Cisco Jabber para Android e iOS, versión 12.9.4.

Detalle:

- La vulnerabilidad crítica se debe a la validación inadecuada del contenido de los mensajes. Un atacante remoto, autenticado, podría explotar esta vulnerabilidad enviando mensajes XMPP, especialmente diseñados, a los productos afectados, resultando en la ejecución de código arbitrario. Se ha asignado el identificador CVE-2020-26085 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2020-27134, CVE-2020-27133, CVE-2020-27132 y CVE-2020-27127.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

Campaña de explotación activa contra SolarWinds Orion Platform

Fecha de publicación: 14/12/2020

Importancia: Crítica

Recursos afectados:

SolarWinds Orion Platform, versiones desde 2019.4 HF 5, hasta 2020.2.1, publicadas entre marzo de 2020 y junio de 2020.

Descripción:

FireEye ha descubierto una campaña de intrusión global y está rastreando a los actores responsables de la misma, como UNC2452. Se recomienda actualizar SolarWinds Orion Platform a la versión 2020.2.1 HF 1 a la mayor brevedad, ya que esta vulnerabilidad podría ser explotada de manera activa.

Solución:

Se recomienda actualizar SolarWinds Orion Platform a la versión 2020.2.1 HF 1 a la mayor brevedad, disponible en *SolarWinds Customer Portal*, ya que esta vulnerabilidad podría ser explotada de manera activa. Si no puede actualizarse inmediatamente, por favor siga las pautas disponibles aquí para asegurar su instancia de SolarWinds Orion Platform.

Si no está seguro de qué versión de Orion Platform está usando, consulte las instrucciones para comprobarlo aquí. Para comprobar qué hotfixes ha aplicado, consúltelo aquí.

Se prevé que el 15 de diciembre de 2020 se publique una nueva versión del *hotfix*, 2020.2.1 HF 2. Se recomienda a todos los clientes que actualicen a la versión 2020.2.1 HF 2 una vez que esté disponible, ya que la versión 2020.2.1 HF 2 reemplaza el componente comprometido y proporciona varias mejoras de seguridad adicionales.

Detalle:

FireEye ha descubierto un ataque a la cadena de suministro que ha troyanizado las actualizaciones del *software* empresarial SolarWinds Orion para distribuir un *malware* tipo *backdoor* denominado SUNBURST. La campaña, cuyos actores responsables son conocidos como UNC2452, está muy extendida y afecta a organizaciones públicas y privadas de todo el mundo.

El *malware* enmascara su tráfico de red como el protocolo OIP (*Orion Improvement Program*) y almacena los resultados del reconocimiento en archivos de configuración de *plugins* legítimos, lo que le permite ocultarse entre la actividad legítima de SolarWinds. El *backdoor* utiliza múltiples listas de bloqueo ofuscadas para identificar las herramientas forenses y antivirus que se ejecutan como procesos, servicios y controladores.

La actividad posterior a este compromiso de la cadena de suministro ha incluido movimiento lateral y robo de datos. FireEye está publicando firmas para detectar esta amenaza.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Virtualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de ABB

Fecha de publicación: 16/12/2020

Importancia: Crítica

Recursos afectados:

- ABB Ability™ Symphony®Plus:
  - S Operations 1.1;
  - S Operations 2.0, todos los Service Packs;
  - S Operations 2.1, Service Pack 1 (SP1), para Melody y otros Heritage systems;
  - S Operations 2.1, Service Pack 2 (SP2);
  - S Operations 3.0;
  - S Operations 3.1;
  - S Operations 3.2;
  - S Operations 3.3.
- ABB Ability™ Symphony®Plus:
  - S Historian 3.0 y 3.1.
- ABB Central Licensing System (CLS) en ABB Ability™ Symphony Plus Operations (desde la 3.0 hasta la 3.3);
- ABB Central Licensing System (CLS) en ABB Ability™ Symphony Plus Engineering (desde la 1.0 hasta la 2.3);
- ABB Central Licensing System (CLS) en Composer Harmony (5.1, 6.0 y 6.1);
- ABB Central Licensing System (CLS) en Composer Melody (5.3 y 6.1);
- ABB Central Licensing System (CLS) en HarmonyOPC Server (6.0, 6.1 y 7.0).

Descripción:

ABB ha publicado múltiples vulnerabilidades que podrían permitir a un atacante abusar de las funcionalidades de los productos afectados

Solución:

- Para S Operations:

    - Actualizar a la versión 3.3 Service Pack 1.
- Para S Operations, versiones anteriores a la 3.X, se preveen tres actualizaciones:
    - Q4 2020: S Operations 2.1 SP 2 Rollup 2 (Harmony, SD y Freelance);
    - Q1 2021: S Operations 2.2 (Melody y Procontrol P14);
    - Q3 2021: S Operations 2.2 Rollup 1 (Procontrol P13).
- Para ABB Ability™ Symphony®Plus:
    - Actualizar a S Historian 3.2.
- Para Sym-phony Plus, Composer Harmony, Composer Melody y HarmonyOPC Server:
    - Actualizar a la última versión disponible y aplicar las medidas de seguridad genéricas, descritas en el aviso 2PAA121231.

Detalle:

- Las vulnerabilidades críticas que afectan al producto ABB Ability™ Symphony®Plus Operations y ABB Ability™ Symphony®Plus Historian, son del tipo:
    - SQL Injection. Se ha asignado el identificador CVE-2020-24673 para esta vulnerabilidad.
    - Método de autenticación débil. Se ha asignado el identificador CVE-2020-24675 para esta vulnerabilidad.
    - Omisión de autenticación. Solo afecta a S Operations. Se ha asignado el identificador CVE-2020-24683 para esta vulnerabilidad.
- Las vulnerabilidades críticas que afectan a los productos Sym-phony Plus, Composer Harmony, Composer Melody y HarmonyOPC Server, son del tipo:
    - XXE. Se ha asignado el identificador CVE-2020-8479 para esta vulnerabilidad.
    - Divulgación de información. Se ha asignado el identificador CVE-2020-8481 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-24674, CVE-2020-24676, CVE-2020-24677, CVE-2020-24678, CVE-2020-24679, CVE-2020-24680, CVE-2020-8481 y CVE-2020-8471.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en HPE Systems Insight Manager (SIM)

Fecha de publicación: 16/12/2020

Importancia: Crítica

Recursos afectados:

HPE Systems Insight Manager (SIM), versiones 7.6.x.

Descripción:

El investigador, Harrison Neal, a través de Trend Micro Zero Day Initiative, ha informado a Hewlett Packard Enterprise de una vulnerabilidad que podría permitir la ejecución remota de código en HPE Systems Insight Manager (SIM).

Solución:

HPE ha informado que publicara una futura versión que corrija esta vulnerabilidad y recomienda seguir los siguientes los pasos para eliminar las funciones "Federated Search" y "Federated CMS Configuration":

1. Detener el servicio HPE SIM.
2. Eliminar el archivo < C:Program FilesHPSystems Insight Managerjbossserverhpsimdeploysimsearch.war > de la ruta de instalación: *del /Q /F C:Program FilesHPSystems Insight Managerjbossserverhpsimdeploysimsearch.war.*
3. Reiniciar el servicio HPE SIM.
4. Esperar a que se pueda acceder a la página web de HPE SIM "https://SIM_IP:50000" y ejecutar el siguiente comando desde el símbolo del sistema: *mxtool -r -f toolsmulti-cms-search.xml 1 >nul 2 >nul.*

Detalle:

Se ha identificado una vulnerabilidad en HPE Systems Insight Manager (SIM) versión 7.6. La vulnerabilidad podría aprovecharse para permitir la ejecución remota de código. Se ha asignado el identificador CVE-2020-7200 para esta vulnerabilidad.

Etiquetas: HP, Vulnerabilidad

Múltiples vulnerabilidades en productos Netgear

Fecha de publicación: 17/12/2020

Importancia: Crítica

Recursos afectados:

- DGN2200v1, con versiones de *firmware* anteriores a la v1.0.0.60;
- SXK80, con versiones de *firmware* anteriores a la 3.1.0.104;
- NMS300, con versiones de *firmware* anteriores a la 1.6.0.27.

Descripción:

Netgear ha publicado varias vulnerabilidades de severidad crítica que afectan a sus productos.

Solución:

Acceder a la página de soporte de Netgear y descargar la última versión del *firmware* del dispositivo afectado.

Detalle:

Las vulnerabilidades son del tipo:

- Vulnerabilidad en la autenticación HTTPd.
- Falta de control de acceso a nivel de función.
- Inyección de comandos previa a la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en HPE iLO Amplifier Pack

Fecha de publicación: 18/12/2020

Importancia: Crítica

Recursos afectados:

iLO Amplifier Pack, versión 1.70.

Descripción:

El investigador, Erik de Jong, ha informado a Hewlett Packard Enterprise de una vulnerabilidad, de severidad crítica, de tipo ejecución remota de código.

Solución:

Actualizar a la versión 1.71.

Detalle:

Una vulnerabilidad de seguridad en el servidor HPE iLO Amplifier Pack podría permitir a un atacante realizar una ejecución remota de código (RCE). Se ha asignado el identificador CVE-2020-7203 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Inyección de comandos en router y sistemas Wi-Fi de Netgear

Fecha de publicación: 23/12/2020

Importancia: Crítica

Recursos afectados:

- R6400v2, con versiones de *firmware* anteriores a 1.0.4.84;
- R6700v3, con versiones de *firmware* anteriores a 1.0.4.84;
- R6900P, con versiones de *firmware* anteriores a 1.3.2.124;
- R7000, con versiones de *firmware* anteriores a 1.0.11.100;
- R7000P, con versiones de *firmware* anteriores a 1.3.2.124;
- R7800, con versiones de *firmware* anteriores a 1.0.2.74;
- R7850, con versiones de *firmware* anteriores a 1.0.5.60;
- R7900, con versiones de *firmware* anteriores a 1.0.4.26;
- R7960P, con versiones de *firmware* anteriores a 1.4.1.50;
- R8000, con versiones de *firmware* anteriores a 1.0.4.52;
- R7900P, con versiones de *firmware* anteriores a 1.4.1.50;
- R8000P, con versiones de *firmware* anteriores a 1.4.1.50;
- RAX15, con versiones de *firmware* anteriores a 1.0.1.64;
- RAX20, con versiones de *firmware* anteriores a 1.0.1.64;
- RAX200, con versiones de *firmware* anteriores a 1.0.1.12;
- RAX45, con versiones de *firmware* anteriores a 1.0.2.66;
- RAX50, con versiones de *firmware* anteriores a 1.0.2.66;
- RAX75, con versiones de *firmware* anteriores a 1.0.3.102;
- RAX80, con versiones de *firmware* anteriores a 1.0.3.102;
- RBK752, con versiones de *firmware* anteriores a 3.2.16.6;
- RBR750, con versiones de *firmware* anteriores a 3.2.16.6;
- RBS750, con versiones de *firmware* anteriores a 3.2.16.6;
- RBK852, con versiones de *firmware* anteriores a 3.2.15.25;
- RBR850, con versiones de *firmware* anteriores a 3.2.15.25;
- RBS850, con versiones de *firmware* anteriores a 3.2.15.25;
- RBK842, con versiones de *firmware* anteriores a 3.2.15.25;

- RBR840, con versiones de *firmware* anteriores a 3.2.15.25;
- RBS840, con versiones de *firmware* anteriores a 3.2.15.25;
- RS400, con versiones de *firmware* anteriores a 1.5.0.48;
- XR300, con versiones de *firmware* anteriores a 1.0.3.50.

Descripción:

Netgear ha publicado una vulnerabilidad de severidad crítica, identificada por el investigador *talsonor*, que afecta a varios de sus productos.

Solución:

Acceder a la página de soporte de Netgear y descargar la última versión del *firmware* de los dispositivos afectados.

Detalle:

Netgear ha publicado correcciones para una vulnerabilidad de seguridad de tipo inyección de comandos previa a la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Dell Wyse ThinOS

Fecha de publicación: 23/12/2020

Importancia: Crítica

Recursos afectados:

Las versiones anteriores a la 8.6 MR8, en las que el cliente recibe configuraciones de un servidor de archivos remoto a través de un protocolo inseguro, de los siguientes productos:

- Dell Wyse 3040 Thin Client (ENG),
- Dell Wyse 3040 Thin Client (JPN),
- Dell Wyse 3040 Thin Client con PCoIP (ENG),
- Dell Wyse 3040 Thin Client con PCoIP (JPN),
- Dell Wyse 5010 Thin Client (ENG),
- Dell Wyse 5010 Thin Client (JPN),
- Dell Wyse 5010 Thin Client con PCoIP (ENG),
- Dell Wyse 5010 Thin Client con PCoIP (JPN),
- Dell Wyse 5040 Thin Client (ENG),
- Dell Wyse 5040 Thin Client (JPN),
- Dell Wyse 5040 Thin Client con PCoIP (ENG),
- Dell Wyse 5040 Thin Client con PCoIP (JPN),
- Dell Wyse 5060 Thin Client (ENG),
- Dell Wyse 5060 Thin Client (JPN),
- Dell Wyse 5060 Thin Client con PCoIP (ENG),
- Dell Wyse 5060 Thin Client con PCoIP (JPN),
- Dell Wyse 5070 Thin Client (ENG),
- Dell Wyse 5070 Thin Client (JPN),
- Dell Wyse 5070 Thin Client con PCoIP (ENG),
- Dell Wyse 5070 Thin Client con PCoIP (JPN),
- Dell Wyse 5470 AIO Thin Client (ENG),
- Dell Wyse 5470 AIO Thin Client (JPN),
- Dell Wyse 5470 AIO Thin Client con PCoIP (ENG),
- Dell Wyse 5470 AIO Thin Client con PCoIP (JPN),
- Dell Wyse 5470 Thin Client (ENG),
- Dell Wyse 5470 Thin Client (JPN),
- Dell Wyse 5470 Thin Client con PCoIP (ENG),
- Dell Wyse 5470 Thin Client con PCoIP (JPN),
- Dell Wyse 7010 Thin Client (ENG),
- Dell Wyse 7010 thin client (JPN).

Descripción:

Se han publicado dos vulnerabilidades, ambas de severidad crítica, en la configuración predeterminada que podrían permitir a un atacante acceder a un archivo de escritura que puede ser usado para manipular la configuración de un cliente específico y obtener acceso a información sensible.

Solución:

Actualizar a las siguientes versiones:

- Dell Wyse 3040 Thin Client (ENG),
- Dell Wyse 3040 Thin Client (JPN),
- Dell Wyse 3040 Thin Client con PCoIP (ENG),
- Dell Wyse 3040 Thin Client con PCoIP (JPN),
- Dell Wyse 5010 Thin Client (ENG),
- Dell Wyse 5010 Thin Client (JPN),
- Dell Wyse 5010 Thin Client con PCoIP (ENG),
- Dell Wyse 5010 Thin Client con PCoIP (JPN),
- Dell Wyse 5040 Thin Client (ENG),
- Dell Wyse 5040 Thin Client (JPN),
- Dell Wyse 5040 Thin Client con PCoIP (ENG),
- Dell Wyse 5040 Thin Client con PCoIP (JPN),

- Dell Wyse 5060 Thin Client (ENG),
- Dell Wyse 5060 Thin Client (JPN),
- Dell Wyse 5060 Thin Client con PCoIP (ENG),
- Dell Wyse 5060 Thin Client con PCoIP (JPN),
- Dell Wyse 5070 Thin Client (ENG),
- Dell Wyse 5070 Thin Client (JPN),
- Dell Wyse 5070 Thin Client con PCoIP (ENG),
- Dell Wyse 5070 Thin Client con PCoIP (JPN),
- Dell Wyse 5470 AIO Thin Client (ENG),
- Dell Wyse 5470 AIO Thin Client (JPN),
- Dell Wyse 5470 AIO Thin Client con PCoIP (ENG),
- Dell Wyse 5470 AIO Thin Client con PCoIP (JPN),
- Dell Wyse 5470 Thin Client (ENG),
- Dell Wyse 5470 Thin Client (JPN),
- Dell Wyse 5470 Thin Client con PCoIP (ENG),
- Dell Wyse 5470 Thin Client con PCoIP (JPN),
- Dell Wyse 7010 Thin Client (ENG),
- Dell Wyse 7010 thin client (JPN).

Detalle:

- Una vulnerabilidad del tipo configuración predeterminada insegura, podría permitir a un atacante remoto, no autenticado, obtener acceso a la información sensible de la red local, lo que llevaría a un posible compromiso de los clientes afectados. Se ha asignado el identificador CVE-2020-29491 para esta vulnerabilidad.
- Una vulnerabilidad del tipo configuración predeterminada insegura, podría permitir a un atacante remoto, no autenticado, acceder al archivo de escritura y manipular la configuración de cualquier estación específica de destino. Se ha asignado el identificador CVE-2020-29492 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Ejecución remota de comandos en la API de SolarWinds Orion

Fecha de publicación: 28/12/2020

Importancia: Crítica

Recursos afectados:

Todas las versiones anteriores a:

- 2019.4 HF 6 (publicada el 14 de diciembre de 2020);
- 2020.2.1 HF 2 (publicada el 15 de diciembre de 2020);
- 2019.2 SUPERNOVA Patch (publicada el 23 de diciembre de 2020);
- 2018.4 SUPERNOVA Patch (publicada el 23 de diciembre de 2020);
- 2018.2 SUPERNOVA Patch (publicada el 23 de diciembre de 2020).

Descripción:

Se ha identificado una vulnerabilidad en la plataforma SolarWinds Orion que permite evadir la autenticación de la API incluida en el producto y facilita a un atacante la ejecución remota de comandos. Esta vulnerabilidad ha sido utilizada por el *malware* conocido como SUPERNOVA.

Este es un problema de seguridad diferente del identificado anteriormente a través de la cadena de suministro en la campaña de explotación contra SolarWinds Orion y que utilizaba la *backdoor* conocida como SUNBURST.

Solución:

Se recomienda actualizar a las siguientes versiones:

- 2019.4 HF 6 (publicada el 14 de diciembre de 2020);
- 2020.2.1 HF 2 (publicada el 15 de diciembre de 2020);
- 2019.2 SUPERNOVA Patch (publicada el 23 de diciembre de 2020);
- 2018.4 SUPERNOVA Patch (publicada el 23 de diciembre de 2020);
- 2018.2 SUPERNOVA Patch (publicada el 23 de diciembre de 2020).

Detalle:

Se ha identificado una vulnerabilidad que permite evadir la autenticación de la API incluida en la plataforma SolarWinds Orion. La vulnerabilidad se produce al incluir parámetros específicos en una solicitud URI dentro de *Request.PathInfo*, permitiendo a un atacante ejecutar comandos de API no autenticados, al obtener la flag *SkipAuthorization* del servidor SolarWinds Orion. Se ha asignado el identificador CVE-2020-10148 a esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de Netgear

Fecha de publicación: 28/12/2020

Importancia: Crítica

Recursos afectados:

- AC2100, ejecutando versiones de firmware anteriores a 1.2.0.72;
- AC2400, ejecutando versiones de firmware anteriores a 1.2.0.72;
- AC2600, ejecutando versiones de firmware anteriores a 1.2.0.72;
- CBK40, ejecutando versiones de firmware anteriores a 2.5.0.10;
- CBR40, ejecutando versiones de firmware anteriores a 2.5.0.10;
- D6000, ejecutando versiones de firmware anteriores a 1.0.0.80;
- D6220, ejecutando versiones de firmware anteriores a 1.0.0.60;
- D6400, ejecutando versiones de firmware anteriores a 1.0.0.94;
- D7000v2, ejecutando versiones de firmware anteriores a 1.0.0.62;
- D7800, ejecutando versiones de firmware anteriores a 1.0.3.48;
- D8500, ejecutando versiones de firmware anteriores a 1.0.3.50;
- DC112A, ejecutando versiones de firmware anteriores a 1.0.0.48;
- DGN2200v4, ejecutando versiones de firmware anteriores a 1.0.0.114;
- DM200, ejecutando versiones de firmware anteriores a 1.0.0.66;
- EAX20, ejecutando versiones de firmware anteriores a 1.0.0.36;
- EAX80, ejecutando versiones de firmware anteriores a 1.0.1.62;
- EX2700, ejecutando versiones de firmware anteriores a 1.0.1.58;
- EX3110, ejecutando versiones de firmware anteriores a 1.0.1.68;
- EX3700, ejecutando versiones de firmware anteriores a 1.0.0.84;
- EX3800, ejecutando versiones de firmware anteriores a 1.0.0.84;
- EX3920, ejecutando versiones de firmware anteriores a 1.0.0.84;
- EX6000, ejecutando versiones de firmware anteriores a 1.0.0.44;
- EX6100v2, ejecutando versiones de firmware anteriores a 1.0.1.94;
- EX6110, ejecutando versiones de firmware anteriores a 1.0.1.68;
- EX6120, ejecutando versiones de firmware anteriores a 1.0.0.54;
- EX6130, ejecutando versiones de firmware anteriores a 1.0.0.36;
- EX6150v1, ejecutando versiones de firmware anteriores a 1.0.0.46;
- EX6150v2, ejecutando versiones de firmware anteriores a 1.0.1.94;
- EX6200v1, ejecutando versiones de firmware anteriores a 1.0.3.94;
- EX6250, ejecutando versiones de firmware anteriores a 1.0.0.128;
- EX6400, ejecutando versiones de firmware anteriores a 1.0.2.152;
- EX6400v2, ejecutando versiones de firmware anteriores a 1.0.0.128;
- EX6410, ejecutando versiones de firmware anteriores a 1.0.0.128;
- EX6920, ejecutando versiones de firmware anteriores a 1.0.0.54;
- EX7000, ejecutando versiones de firmware anteriores a 1.0.1.90;
- EX7300, ejecutando versiones de firmware anteriores a 1.0.2.152;
- EX7300v2, ejecutando versiones de firmware anteriores a 1.0.0.128;
- EX7320, ejecutando versiones de firmware anteriores a 1.0.0.128;
- EX7500, ejecutando versiones de firmware anteriores a 1.0.0.68;
- EX7700, ejecutando versiones de firmware anteriores a 1.0.0.210;
- EX8000, ejecutando versiones de firmware anteriores a 1.0.1.224;
- MK62, ejecutando versiones de firmware anteriores a 1.0.5.102;
- MR60, ejecutando versiones de firmware anteriores a 1.0.5.102;
- MS60, ejecutando versiones de firmware anteriores a 1.0.5.102;
- R6120, ejecutando versiones de firmware anteriores a 1.0.0.70;
- R6220, ejecutando versiones de firmware anteriores a 1.1.0.100;
- R6230, ejecutando versiones de firmware anteriores a 1.1.0.100;
- R6250, ejecutando versiones de firmware anteriores a 1.0.4.42;
- R6260, ejecutando versiones de firmware anteriores a 1.1.0.76;
- R6300v2, ejecutando versiones de firmware anteriores a 1.0.4.42;
- R6330, ejecutando versiones de firmware anteriores a 1.1.0.76;
- R6350, ejecutando versiones de firmware anteriores a 1.1.0.76;
- R6400v1, ejecutando versiones de firmware anteriores a 1.0.1.62;
- R6400v2, ejecutando versiones de firmware anteriores a 1.0.4.98;
- R6700v1, ejecutando versiones de firmware anteriores a 1.0.2.16;
- R6700v2, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R6700v3, ejecutando versiones de firmware anteriores a 1.0.4.98;
- R6800, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R6850, ejecutando versiones de firmware anteriores a 1.1.0.76;
- R6900, ejecutando versiones de firmware anteriores a 1.0.2.16;
- R6900P, ejecutando versiones de firmware anteriores a 1.3.2.124;
- R7000, ejecutando versiones de firmware anteriores a 1.0.11.106;
- R7000P, ejecutando versiones de firmware anteriores a 1.3.2.124;
- R7100LG, ejecutando versiones de firmware anteriores a 1.0.0.56;
- R7500v2, ejecutando versiones de firmware anteriores a 1.0.3.48;
- R7800, ejecutando versiones de firmware anteriores a 1.0.2.74;
- R7850, ejecutando versiones de firmware anteriores a 1.0.5.60;
- R7900, ejecutando versiones de firmware anteriores a 1.0.4.26;
- R7900P, ejecutando versiones de firmware anteriores a 1.4.1.62;
- R7960P, ejecutando versiones de firmware anteriores a 1.4.1.62;
- R8000, ejecutando versiones de firmware anteriores a 1.0.4.58;
- R8000P, ejecutando versiones de firmware anteriores a 1.4.1.62;
- R8300, ejecutando versiones de firmware anteriores a 1.0.2.134;
- R8500, ejecutando versiones de firmware anteriores a 1.0.2.134;
- R8900, ejecutando versiones de firmware anteriores a 1.0.5.24;
- RAX120, ejecutando versiones de firmware anteriores a 1.0.1.136;
- RAX15, ejecutando versiones de firmware anteriores a 1.0.1.64;
- RAX20, ejecutando versiones de firmware anteriores a 1.0.1.64;
- RAX200, ejecutando versiones de firmware anteriores a 1.0.5.24;
- RAX35, ejecutando versiones de firmware anteriores a 1.0.3.80;
- RAX40, ejecutando versiones de firmware anteriores a 1.0.3.80;

- RAX45, ejecutando versiones de firmware anteriores a 1.0.2.64;
- RAX50, ejecutando versiones de firmware anteriores a 1.0.2.64;
- RAX75, ejecutando versiones de firmware anteriores a 1.0.3.102;
- RAX80, ejecutando versiones de firmware anteriores a 1.0.3.102;
- RBK12, ejecutando versiones de firmware anteriores a 2.6.1.44;
- RBR10, ejecutando versiones de firmware anteriores a 2.6.1.44;
- RBS10, ejecutando versiones de firmware anteriores a 2.6.1.44;
- RBK20, ejecutando versiones de firmware anteriores a 2.6.1.38;
- RBR20, ejecutando versiones de firmware anteriores a 2.6.1.36;
- RBS20, ejecutando versiones de firmware anteriores a 2.6.1.38;
- RBK40, ejecutando versiones de firmware anteriores a 2.6.1.38;
- RBR40, ejecutando versiones de firmware anteriores a 2.6.1.38;
- RBS40, ejecutando versiones de firmware anteriores a 2.6.1.38;
- RBK50, ejecutando versiones de firmware anteriores a 2.6.1.40;
- RBR50, ejecutando versiones de firmware anteriores a 2.6.1.40;
- RBS50, ejecutando versiones de firmware anteriores a 2.6.1.40;
- RBR840, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBS840, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBR850, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBS850, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBS40V, ejecutando versiones de firmware anteriores a 2.5.1.6;
- RBS40V-200, ejecutando versiones de firmware anteriores a 1.0.0.46;
- RBS50Y, ejecutando versiones de firmware anteriores a 2.6.1.40;
- RBW30, ejecutando versiones de firmware anteriores a 2.5.0.4;
- RS400, ejecutando versiones de firmware anteriores a 1.5.0.48;
- WN2500RPv2, ejecutando versiones de firmware anteriores a 1.0.1.56;
- WN3000RPv3, ejecutando versiones de firmware anteriores a 1.0.2.86;
- WN3500RPv1, ejecutando versiones de firmware anteriores a 1.0.0.28;
- WNDR3400v3, ejecutando versiones de firmware anteriores a 1.0.1.32;
- WNR1000v3, ejecutando versiones de firmware anteriores a 1.0.2.78;
- WNR2000v2, ejecutando versiones de firmware anteriores a 1.2.0.12;
- XR300, ejecutando versiones de firmware anteriores a 1.0.3.50;
- XR450, ejecutando versiones de firmware anteriores a 2.3.2.66;
- XR500, ejecutando versiones de firmware anteriores a 2.3.2.66;
- XR700, ejecutando versiones de firmware anteriores a 1.0.1.34;
- D7800, ejecutando versiones de firmware anteriores a 1.0.1.58;
- R6400, ejecutando versiones de firmware anteriores a 1.0.1.62;
- R6700, ejecutando versiones de firmware anteriores a 1.0.2.16;
- R6900v2, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R7200, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R7350, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R7400, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R7450, ejecutando versiones de firmware anteriores a 1.2.0.72;
- R9000, ejecutando versiones de firmware anteriores a 1.0.5.24;
- RAX200, ejecutando versiones de firmware anteriores a 1.0.2.102;
- RBK752, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBR750, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBS750, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBK842, ejecutando versiones de firmware anteriores a 3.2.16.6;
- RBK852, ejecutando versiones de firmware anteriores a 3.2.16.6;
- EX6100, ejecutando versiones de firmware anteriores a 1.0.2.28;
- EX6150, ejecutando versiones de firmware anteriores a 1.0.0.46;
- EX6200, ejecutando versiones de firmware anteriores a 1.0.3.94;
- MK62, ejecutando versiones de firmware anteriores a 1.0.4.98;
- MR60, ejecutando versiones de firmware anteriores a 1.0.4.98;
- MS60, ejecutando versiones de firmware anteriores a 1.0.4.98;
- RAX45, ejecutando versiones de firmware anteriores a 1.0.2.32;
- RAX50, ejecutando versiones de firmware anteriores a 1.0.2.32;
- WN3500RP, ejecutando versiones de firmware anteriores a 1.0.0.28;
- WNR3500Lv2, ejecutando versiones de firmware anteriores a 1.2.0.62;
- XR300, ejecutando versiones de firmware anteriores a 1.0.3.50.

Descripción:

Netgear ha publicado 3 vulnerabilidades de severidad crítica, descubiertas por los investigadores, Florian Hehenberger y Simon Birngruber, pertenecientes a la Universidad de Ciencias Aplicadas de Alta Austria, *talsonor* y SSD Secure Disclosure.

Solución:

Acceder a la página de soporte de Netgear y descargar la última versión del firmware de los dispositivos afectados.

Detalle:

Netgear ha publicado actualizaciones para corregir configuraciones de seguridad erróneas, desbordamiento de búfer previo a la autenticación e inyección de comandos previo a la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Veritas

Fecha de publicación: 28/12/2020

Importancia: Crítica

Recursos afectados:

- Backup Exec, versiones BE 20.x, BE 21.x y 16.x. También pueden verse afectadas las versiones anteriores carentes de soporte.
- Veritas System Recovery (VSR), solo las versiones para Windows: 21.1, 21, 18.0.4, 18.0.3, 18.0.2, 18.0.1, 18.0, 16.0.2, 16.0.1 y 16. También pueden verse afectadas las versiones anteriores carentes de soporte.
- NetBackup y OpsCenter, versiones 8.3.0.1 y anteriores. Solo afecta a la plataforma Windows.
- VRP/NetBackup Resiliency Platform, versiones 3.4 y 3.5. También pueden verse afectadas las versiones anteriores carentes de soporte.
- Veritas InfoScale, versiones para Windows: 7.4.2, 7.4.1, 7.4, 7.3.1, 7.3, 7.2, 7.1, 7.0.1 y 7.0; Storage Foundation HA para Windows 6.1; y Storage Foundation para Windows 6.1. También pueden verse afectadas las versiones anteriores carentes de soporte.
- Veritas InfoScale Operations Manager (VIOM), versiones para Windows Management Server: 7.4.2, 7.4, 7.3.1, 7.3, 7.2, 7.1 y 7.0. También pueden verse afectadas las versiones anteriores carentes de soporte.
- Enterprise Vault, versiones 14.0, 12.5.2, 12.5.1, 12.5. 12.4.2. 12.4.1. 12.4, 12.3.2, 12.3.1, 12.3, 12.2.3, 12.2.2, 12.2.1, 12.2, 12.1.3, 12.1.2, 12.1.1, 12.1, 12.0.4, 12.0.3, 12.0.2, 12.0.1 y 12.0. También pueden verse afectadas las versiones anteriores carentes de soporte.
- Veritas Desktop and Laptop Option (DLO), versiones 9.3.3, 9.3.2, 9.3.1, 9.3, 9.2, 9.1, 9.0.1, 9.0 y anteriores a 9.5. También pueden verse afectadas las versiones anteriores carentes de soporte.
- NetBackup con CloudPoint, versiones 8.3.0.1 y 8.3.
- CloudPoint, versiones 2.2.2, 2.2.1, 2.2, 2.1.2, 2.1.1, 2.1, 2.0.2, 2.0.1, 2.0, 1.0.2 y 1.0.
- APTARE IT Analytics, versiones 10.5 y 10.4.

Descripción:

Veritas ha publicado varios avisos que comprenden 11 vulnerabilidades, 10 críticas y 1 media, estando todas las críticas relacionadas con librerías de OpenSSL.

Solución:

Aplicar las actualizaciones:

- Backup Exec 21.1 Hotfix 657517 (versión 21.0.1200.1217);
- Backup Exec 20.6 Hotfix 298543 (versión 20.0.1188.2734);
- Para las versiones Backup Exec 16.X y anteriores: el fabricante recomienda actualizar a la versión Backup Exec 21.2.
- Veritas System Recovery (VSR) 21.2;
- OpenSSL Hotfix para NetBackup 8.1.2, NetBackup 8.2, NetBackup 8.3 o NetBackup 8.3.0.1;
- VRP/NetBackup Resiliency Platform v3.6 (disponible en enero de 2021) o aplicar el parche para v3.4 o v3.5;
- Veritas Desktop and Laptop Option (DLO) versión 9.5;
- NetBackup 8.3.0.1 y aplicar el HotFix para NetBackup junto con los componentes de CloudPoint.

Estos *hotfix* estarán disponibles en el centro de descargas de Veritas para su descarga e instalación automática.

Como medida de mitigación alternativa para el producto Backup Exec, es posible crear, mediante una cuenta de administrador, el directorio 'usrlocalssl' bajo la raíz de todas las unidades y establecer el ACL en el directorio para negar el acceso de escritura a todos los demás usuarios. Esto evitará que un atacante instale un motor OpenSSL malicioso.

Detalle:

Un atacante con pocos privilegios en el sistema Windows y sin ningún privilegio en alguno de los productos afectados, podría crear un archivo de configuración especialmente diseñado, en una ruta específica, para cargar un motor OpenSSL malicioso y ejecutar código arbitrario como SYSTEM, cuando el servicio se inicia. Esto le otorgaría al atacante acceso de administrador en el sistema, permitiendo al atacante (por defecto) acceder a todos los datos, a todas las aplicaciones instaladas, etc. Si el sistema es también un controlador de dominio de Active Directory, esto podría afectar a todo el dominio.

Se ha asignado el identificador CVE-2019-12572 para esta vulnerabilidad en el producto Backup Exec.

Etiquetas: Actualización, SSL/TLS, Vulnerabilidad

Ataque DDoS amplificado contra Citrix ADC y Gateway

Fecha de publicación: 28/12/2020

Importancia: Alta

Recursos afectados:

- Citrix ADC (*Application Delivery Controller*),
- Citrix Gateway.

En este momento, el alcance del ataque se limita a un pequeño número de clientes en todo el mundo.

Descripción:

Citrix ha detectado un patrón de ataques DDoS que están utilizando el protocolo DTLS (*Datagram Transport Layer Security*) como vector de amplificación.

Solución:

Citrix está trabajando en una mejora de las características del protocolo DTLS para eliminar la susceptibilidad a este ataque y espera tener esta mejora disponible en la página de descargas de Citrix para todas las versiones soportadas el 12 de enero de 2021. Hasta ese momento, se recomienda deshabilitar DTLS a través del siguiente comando CLI:

```
set vpn vserver < vpn_vserver_name > -dtls OFF
```

Si está ejecutando alguna aplicación que deba usar EDT (*Enlightened Data Transport*), o si no puede desactivar el DTLS, póngase en contacto con el Soporte Técnico de Citrix para hablar de su entorno.

Detalle:

Un atacante podría sobrecargar el rendimiento de la red DTLS de Citrix ADC, lo que podría llevar a un agotamiento del ancho de banda de salida. El efecto de este ataque parece ser más prominente en conexiones con un ancho de banda limitado. Para determinar si un ADC es objetivo de este ataque, se debe monitorizar el volumen de tráfico de salida para detectar cualquier anomalía significativa o picos.

Etiquetas: Comunicaciones