
# Boletín de abril de 2021

## Avisos Técnicos

## Vulnerabilidad de gestión incorrecta de URL en VMware Carbon Black Cloud Workload

**Fecha de publicación:** 05/04/2021

**Importancia:** Crítica

**Recursos afectados:**

VMware Carbon Black Cloud Workload, versión 1.0.1 y anteriores ejecutándose en sistemas Linux.

**Descripción:**

Egor Dimitrenko, investigador de Positive Technologies, ha reportado a VMware una vulnerabilidad, con severidad crítica, en la que un atacante podría realizar una escalada de privilegios debido a una gestión incorrecta de URL.

**Solución:**

Actualizar VMware Carbon Black Cloud Workload a la versión 1.0.2.

**Detalle:**

Un atacante, con acceso de red a la interfaz administrativa del dispositivo VMware Carbon Black Cloud Workload, podría obtener un *token* de autenticación válido, concediendo acceso a la API de administración del dispositivo. La explotación exitosa de esta vulnerabilidad podría permitir al atacante ver y alterar los ajustes de configuración administrativa. Se ha asignado el identificador CVE-2021-21982 para esta vulnerabilidad.

**Etiquetas:** Actualización, Virtualización, VMware, Vulnerabilidad

## Múltiples vulnerabilidades en varios productos de Cisco

**Fecha de publicación:** 08/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- Rúters Cisco Small Business:
  - RV110W Wireless-N VPN Firewall;
  - RV130 VPN Router;
  - RV130W Wireless-N Multifunction VPN Router;
  - RV215W Wireless-N VPN Router.
- Software SD-WAN vManage, versión 18.4 y anteriores, 19.2, 19.3, 20.1, 20.3 y 20.4.

**Descripción:**

Se han identificado 2 vulnerabilidades de severidad crítica y otras 2 de severidad alta que podrían permitir a un atacante, remoto y no autenticado, realizar una escalada de privilegios o ejecutar código arbitrario.

**Solución:**

En el caso del Software SD-WAN vManage, se recomienda actualizar a las versiones estables 19.2.4, 20.3.3 y 20.4.1 respectivamente.

En el caso de los rúters, se recomienda migrar a los productos RV132W, RV160 o RV160W, ya que no se publicarán actualizaciones al haber alcanzado el fin de su vida útil.

**Detalle:**

Las vulnerabilidades críticas se refieren a:

- La validación incorrecta de los datos de entrada en el gestor remoto del software SD-WAN vManage podría permitir a un atacante, remoto y no autenticado, ocasionar una condición de desbordamiento de búfer y ejecutar código arbitrario en el sistema operativo subyacente con privilegios de *root*, tras el envío de una solicitud de conexión especialmente diseñada. Se ha asignado el identificador CVE-2021-1479 para esta vulnerabilidad crítica.
- La validación incorrecta de los datos de entrada en la interfaz de administración basada en web de los rúters afectados podría permitir a un atacante, remoto y no autenticado, ejecutar código arbitrario como usuario *root* en el sistema operativo subyacente, mediante el envío de solicitudes HTTP especialmente diseñadas. Se ha asignado el identificador CVE-2021-1459 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades, de severidad alta, se han asignado los identificadores CVE-2021-1137 y CVE-2021-1480.

**Etiquetas:** Actualización, Cisco, Comunicaciones, Vulnerabilidad

---

# Múltiples vulnerabilidades en varios productos de Synology

**Fecha de publicación:** 12/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- DiskStation Manager (DSM), versión 6.2;
- DSM UC, versión 3.0;
- SkyNAS;
- VS960HD.

**Descripción:**

Se han identificado 6 vulnerabilidades de severidad crítica y otras 6 de severidad alta que podrían permitir a un atacante remoto ejecutar código arbitrario.

**Solución:**

En el caso del producto DSM, actualizar a la versión 6.2.3-25426-3 u otra superior.

Para el resto de productos, no existe una solución por el momento.

**Detalle:**

- Una vulnerabilidad de condición de carrera, una vulnerabilidad de tipo *Use-After-Free* o una vulnerabilidad de lectura fuera de límites en *iscsi_snapshot_comm_core* de DSM, podrían permitir a un atacante remoto ejecutar código arbitrario a través de solicitudes web especialmente diseñadas. Se han asignado los identificadores CVE-2021-26569, CVE-2021-27646 y CVE-2021-27647 para estas vulnerabilidades críticas.
- Una vulnerabilidad de transmisión de texto sin cifrar con información confidencial, una vulnerabilidad de desbordamiento de búfer basada en pila (*stack*) o una vulnerabilidad de escritura fuera de límites en *synoagentregisterd* de DSM, podrían permitir ataques de *man-in-the-middle* para falsificar servidores o ejecutar código arbitrario respectivamente. Se han asignado los identificadores CVE-2021-26560, CVE-2021-26561 y CVE-2021-26562 para estas vulnerabilidades críticas.

Para el resto de vulnerabilidades se han asignado los identificadores CVE-2021-26563, CVE-2021-26564, CVE-2021-26565, CVE-2021-26566, CVE-2021-26567 y CVE-2021-29083.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

---

# Actualizaciones de seguridad de Microsoft de abril de 2021

**Fecha de publicación:** 14/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- Azure AD Web Sign-in,
- Azure DevOps,
- Azure Sphere,
- Microsoft Edge (basado en Chromium),
- Microsoft Exchange Server,

- Microsoft Graphics Component,
- Microsoft Internet Messaging API,
- Microsoft NTFS,
- Microsoft Office Excel,
- Microsoft Office Outlook,
- Microsoft Office SharePoint,
- Microsoft Office Word,
- Microsoft Windows Codecs Library,
- Microsoft Windows Speech,
- Open Source Software,
- Role: DNS Server,
- Role: Hyper-V,
- Visual Studio,
- Visual Studio Code,
- Visual Studio Code - GitHub Pull Requests e Issues Extension,
- Visual Studio Code - Kubernetes Tools,
- Visual Studio Code - Maven para Java Extension,
- Windows Application Compatibility Cache,
- Windows AppX Deployment Extensions,
- Windows Console Driver,
- Windows Diagnostic Hub,
- Windows Early Launch Antimalware Driver,
- Windows ELAM,
- Windows Event Tracing,
- Windows Installer,
- Windows Kernel,
- Windows Media Player,
- Windows Network File System,
- Windows Overlay Filter,
- Windows Portmapping,
- Windows Registry,
- Windows Remote Procedure Call Runtime,
- Windows Resource Manager,
- Windows Secure Kernel Mode,
- Windows Services and Controller App,
- Windows SMB Server,
- Windows TCP/IP,
- Windows Win32K,
- Windows WLAN Auto Config Service.

**Descripción:**

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de abril, consta de 117 vulnerabilidades, clasificadas 19 como críticas, 89 como importantes y 9 sin severidad asignada.

**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:

- Denegación de servicio.
- Escalada de privilegios.
- Divulgación de información.
- Ejecución remota de código.
- Omisión de la función de seguridad.
- Suplantación de identidad (*spoofing*).

Microsoft también ha corregido hoy 5 vulnerabilidades 0day con identificadores CVE-2021-27091, CVE-2021-28312, CVE-2021-28437, CVE-2021-28458 y CVE-2021-28310 (esta última estaba siendo explotada activamente).

**IMPORTANTE**: la NSA ha notificado 4 vulnerabilidades críticas de ejecución remota de código que afectan a Microsoft Exchange Server (2013, 2016 y 2019) y que han sido solucionadas en este boletín (2013 CU23; 2016 CU19 y CU20, y 2019 CU8 y CU9). Sus identificadores son CVE-2021-28480, CVE-2021-28481, CVE-2021-28482 y CVE-2021-28483.

**Etiquetas:** 0day, Actualización, Comunicaciones, DNS, Infraestructuras críticas, Navegador, Privacidad, Virtualización, Vulnerabilidad, Windows

---

# NAME:WRECK, múltiples vulnerabilidades en DNS

**Fecha de publicación:** 14/04/2021

**Importancia:** Crítica

**Recursos afectados:**

Implementaciones DNS en las pilas TCP/IP: FreeBSD, Nucleus NET, IPnet y NetX.

**Descripción:**

Forescout Research Labs, en colaboración con JSOF Research, ha revelado NAME:WRECK, un conjunto de nueve vulnerabilidades que afectan a cuatro populares pilas TCP/IP (FreeBSD, Nucleus NET, IPnet y NetX). Estas vulnerabilidades

están relacionadas con las implementaciones del Sistema de Nombres de Dominio (DNS), pudiendo provocar una denegación de servicio (DoS) o una ejecución remota de código (RCE), lo que permitiría a los atacantes desconectar los dispositivos objetivo o tomar el control de los mismos.

**Solución:**

- La protección completa contra NAME:WRECK requiere parchear los dispositivos que ejecutan las versiones vulnerables de las pilas IP. FreeBSD, Nucleus NET y NetX han sido parcheados recientemente, y los proveedores de dispositivos que utilizan este software deberían proporcionar sus propias actualizaciones a los clientes. Es posible que estas actualizaciones en los diferentes clientes se alarguen en el tiempo y no se publiquen de manera inmediata, debido a la complejidad de las mismas y a las diferentes casuísticas. Se recomienda a cualquiera que utilice un producto que incorpore servicios para la resolución de DNS o DHCP revise las actualizaciones de su fabricante que se puedan producir a lo largo del tiempo y que permitirían corregir estas vulnerabilidades.

Sin embargo, no siempre es posible parchear los dispositivos, y el esfuerzo requerido cambia drásticamente dependiendo de si el dispositivo es un servidor de TI estándar o un dispositivo IoT. Teniendo en cuenta estos desafíos, se recomienda la siguiente estrategia de mitigación:

- Realizar un inventario de los dispositivos que ejecutan las pilas vulnerables. Forescout Research Labs ha publicado un script de código abierto que utiliza la huella digital activa para detectar los dispositivos que ejecutan las pilas afectadas. El script se actualiza constantemente con nuevas firmas para seguir el último desarrollo de su investigación. Los clientes de Forescout que utilizan eyeSight también pueden identificar automáticamente los dispositivos que utilizan FreeBSD, Nucleus RTOS, ThreadX o VxWorks.
- Aplicar controles de segmentación y un bastionado de red adecuado para mitigar el riesgo de los dispositivos vulnerables. Restrinja las vías de comunicación externas y aísle o contenga los dispositivos vulnerables en zonas como control de mitigación si no pueden ser parcheados o hasta que puedan serlo.
- Supervisar los parches progresivos publicados por los proveedores de dispositivos afectados y diseñar un plan de recuperación para su inventario de activos vulnerables, equilibrando el riesgo empresarial y los requisitos de continuidad del negocio.
- Configurar los dispositivos para que dependan de los servidores DNS internos en la medida de lo posible y supervisar detalladamente el tráfico DNS externo, ya que la explotación requiere que un servidor DNS malicioso responda con paquetes maliciosos.
- Supervisar todo el tráfico de red en busca de paquetes maliciosos que intenten explotar vulnerabilidades conocidas o posibles *0-days* que afecten a los clientes DNS, mDNS y DHCP. El tráfico anómalo y malformado debería bloquearse, o al menos debería alertarse de su presencia a los operadores de la red. Para explotar las vulnerabilidades de NAME:WRECK, un atacante debería adoptar un procedimiento similar para cualquier pila TCP/IP. Esto significa que la misma técnica de detección utilizada para identificar la explotación de NAME:WRECK también funcionará para detectar la explotación en otras pilas TCP/IP y productos que aún no han sido analizadas. Además, los clientes de Forescout eyeInspect que activaron el script SD de detección de amenazas entregado como parte de AMNESIA:33 pueden detectar la explotación de NAME:WRECK.

**Detalle:**

- Un error de límite al analizar los datos de la opción 119 en los paquetes DHCP en *dhclient(8)*, podría permitir a un atacante remoto, en la red local, enviar datos especialmente diseñados al cliente DHCP, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino. Se ha asignado el identificador CVE-2020-7461 para esta vulnerabilidad.
- El desbordamiento basado en la pila en la función de descompresión de mensajes del cliente DNS, podría permitir a un atacante la ejecución remota de código (RCE). Se ha asignado el identificador CVE-2016-20009 para esta vulnerabilidad, que es la de mayor severidad con un CVSS de 9.8.
- La funcionalidad de análisis de etiquetas de nombres de dominio DNS no valida correctamente los nombres en las respuestas DNS. El análisis sintáctico de respuestas malformadas podría dar lugar a una escritura más allá del final de una estructura asignada. Un atacante con una posición privilegiada en la red podría aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual o provocar una condición de denegación de servicio. Se ha asignado el identificador CVE-2020-15795 para esta vulnerabilidad.
- La funcionalidad de descompresión de registros de nombres de dominio DNS no valida correctamente los valores de desplazamiento del puntero. Un atacante podría elaborar un paquete de respuesta DNS especialmente diseñado que permitiría escribir datos arbitrarios en partes sensibles de la memoria de un dispositivo, donde posteriormente inyectaría el código. Se ha asignado el identificador CVE-2020-27009 para esta vulnerabilidad.
- La funcionalidad de análisis de etiquetas de nombres de dominio DNS no valida correctamente el nombre en las respuestas DNS. El análisis de respuestas malformadas podría dar lugar a una lectura más allá del final de una estructura asignada. Un atacante con una posición privilegiada en la red podría aprovechar esta vulnerabilidad para provocar una condición de denegación de servicio. Se ha asignado el identificador CVE-2020-27736 para esta vulnerabilidad.
- La funcionalidad de análisis de la respuesta DNS no valida correctamente varias longitudes y recuentos de los registros. El análisis sintáctico de respuestas malformadas podría dar lugar a una lectura más allá del final de una estructura asignada. Un atacante con una posición privilegiada en la red podría aprovechar esta vulnerabilidad para provocar una condición de denegación de servicio. Se ha asignado el identificador CVE-2020-27737 para esta vulnerabilidad.
- La funcionalidad de descompresión de registros de nombres de dominio DNS no valida correctamente los valores de desplazamiento del puntero. El análisis sintáctico de respuestas malformadas podría dar lugar a un acceso de lectura más allá del final de una estructura asignada. Un atacante con una posición privilegiada en la red podría aprovechar esta vulnerabilidad para causar una condición de denegación de servicio. Se ha asignado el identificador CVE-2020-27738 para esta vulnerabilidad.
- El cliente DNS no aleatoriza correctamente el ID de transacción DNS (TXID) y los números de puerto UDP, lo que podría permitira un atacante realizar ataques de envenenamiento de caché DNS/suplantación de identidad. Se ha asignado el identificador CVE-2021-25677 para esta vulnerabilidad.
- En el componente DNS resolver, las funciones *_nx_dns_name_string_unencode* y *_nx_dns_resource_name_real_size_calculated* no comprueban que el puntero de compresión no sea igual al mismo desplazamiento que se está analizando actualmente, lo que podría llevar a un bucle infinito. En la función *_nx_dns_resource_name_real_size_calculate* el puntero también puede apuntar hacia adelante y no hay una comprobación de fuera de límites en el búfer del paquete. Aún no se ha asignado ningún identificador para esta vulnerabilidad.

Los detalles de estas vulnerabilidades se describen en el informe técnico y serán presentados en Black Hat Asia 2021.

**Etiquetas:** Actualización, Comunicaciones, DNS, IoT, Vulnerabilidad

# Actualización de seguridad de SAP de abril de 2021

**Fecha de publicación:** 14/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- SAP Business Client, versión 6.5;
- SAP Commerce, versiones 1808, 1811, 1905, 2005 y 2011;
- SAP NetWeaver AS JAVA (MigrationService), versiones 7.10, 7.11, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver Master Data Management, versiones 710 y 710.750;
- SAP Solution Manager, versión 7.20;
- SAP NetWeaver AS for ABAP, versiones 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731 y 2011_1_752, 2020, 731, 740, 750 y 7.30;
- SAP S4 HANA (SAP Landscape Transformation) , versiones 101, 102, 103, 104 y 105;
- SAP Setup, versión 9.0;
- SAP NetWeaver AS for JAVA (Telnet Commands):
  - ENGINEAPI, versiones 7.30, 7.31, 7.40 y 7.50;
  - ESP_FRAMEWORK, versiones 7.10, 7.20, 7.30, 7.31, 7.40 y 7.50;
  - SERVERCORE, versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
  - J2EE-FRMW, versiones 7.10, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver AS for JAVA (Applications based on HTMLB for Java):
  - EP-BASIS, versiones 7.10, 7.11, 7.30, 7.31, 7.40 y 7.50;
  - FRAMEWORK-EXT , versiones 7.30, 7.31, 7.40 y 7.50;
  - FRAMEWORK, versiones 7.10 y 7.11;
- SAP NetWeaver AS for JAVA (Customer Usage Provisioning Servlet), versiones 7.31, 7.40 y 7.50;
- SAP Process Integration, versiones 7.10, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP Manufacturing Execution, versiones 15.1, 15.2, 15.3 y 15.4;
- SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java), versiones 7.00, 7.10, 7.11, 7.20, 7.30, 731, 7.40 y 7.50;
- SAP Focused RUN, versiones 200 y 300;
- SAP NetWeaver AS for JAVA (HTTP Service), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP Fiori Apps 2.0 for Travel Management in SAP ERP, versión 608.

**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 14 notas de seguridad y 5 actualizaciones de notas anteriores, siendo 3 de severidad crítica, 5 de severidad alta y 11 de severidad media.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 2 vulnerabilidades de XSS (*Cross Site Scripting*).
- 1 vulnerabilidad de denegación de servicio (DoS).
- 5 vulnerabilidades de revelación de información.
- 5 vulnerabilidades de falta de comprobación de autenticación.
- 1 vulnerabilidad de ejecución remota de código.
- 5 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- SAP Commerce. Se corrige una vulnerabilidad de ejecución remota de código que podría permitir a un atacante no autorizado explotar las capacidades de scripting del motor de reglas para inyectar código malicioso en las reglas de origen, y permitir así la ejecución remota de código. Se ha asignado el identificador CVE-2021-27602 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2021-21481, CVE-2021-21482, CVE-2021-21483, CVE-2020-26832, CVE-2021-27608, CVE-2021-21485, CVE-2021-27598, CVE-2021-27603, CVE-2021-27599, CVE-2021-27604, CVE-2021-27600, CVE-2021-27601, CVE-2021-21491, CVE-2021-27609, CVE-2021-21492 y CVE-2021-27605.

**Etiquetas:** Actualización, SAP, Vulnerabilidad

# Actualización de seguridad 5.7.1 para WordPress

**Fecha de publicación:** 15/04/2021

**Importancia:** Alta

**Recursos afectados:**

WordPress, todas las versiones anteriores a la 5.7.1.

**Descripción:**

Se ha publicado la última versión de WordPress que corrige 26 errores y 2 problemas de seguridad.

**Solución:**

Actualizar a la versión 5.7.1.

**Detalle:**

Las correcciones de seguridad solucionan las siguientes vulnerabilidades:

- XXE (*XML External Entity*) en la biblioteca multimedia que afecta a PHP 8.
- Exposición de datos en el REST API.

**Etiquetas:** Actualización, CMS, PHP, Vulnerabilidad

---

# Múltiples vulnerabilidades en GitLab y Ruby

**Fecha de publicación:** 15/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- GitLab Community Edition (CE)/Enterprise Edition (EE), versión 11.9 y posteriores.
- Ruby, versiones:
  - 2.5.8 o anteriores,
  - 2.6.7 o anteriores,
  - 2.7.2 o anteriores,
  - 3.0.1 o anteriores.
- REXML gem, versión 3.2.4 o anteriores.

**Descripción:**

Los investigadores, *vakzz* y Juho Nurminen, ambos a través del programa de *bug bounty* de HackerOne, han detectado 2 vulnerabilidades críticas que afectan a GitLab y REXML, de tipo ejecución remota de código (RCE) y conversión de documentos XML, respectivamente.

**Solución:**

Actualizar a:

- GitLab CE/EE, versiones 13.10.3, 13.9.6 y 13.8.8.
- REXML gem a la versión 3.2.5 o posteriores.

**Detalle:**

- Se ha descubierto una vulnerabilidad en GitLab CE/EE por la que no se validaban correctamente los archivos de imagen que se pasaban a un analizador de archivos, lo que daba lugar a la ejecución remota de comandos.
- Al parsear y serializar un documento XML especialmente diseñado, REXML gem (también el que se incluye con Ruby) puede crear un documento XML erróneo cuya estructura es diferente a la original. Se ha asignado el identificador CVE-2021-28965 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Ejecución remota de código en el servicio overlayd de productos Juniper

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- Juniper Networks Junos OS, versiones:
  - 15.1, anteriores a 15.1R7-S9;
  - 17.3, anteriores a 17.3R3-S11;
  - 17.4, anteriores a 17.4R2-S13 y 17.4R3-S4;
  - 18.1, anteriores a 18.1R3-S12;
  - 18.2, anteriores a 18.2R2-S8 y 18.2R3-S7;
  - 18.3, anteriores a 18.3R3-S4;
  - 18.4, anteriores a 18.4R1-S8, 18.4R2-S7 y 18.4R3-S7;
  - 19.1, anteriores a 19.1R2-S2 y 19.1R3-S4;
  - 19.2, anteriores a 19.2R1-S6 y 19.2R3-S2;
  - 19.3, anteriores a 19.3R3-S1;
  - 19.4, anteriores a 19.4R2-S4 y 19.4R3-S1;
  - 20.1, anteriores a 20.1R2-S1 y 20.1R3;
  - 20.2, anteriores a 20.2R2, 20.2R2-S1 y 20.2R3;
  - 20.3, anteriores a 20.3R1-S1.

**Descripción:**

Se ha publicado una vulnerabilidad de validación incorrecta del tamaño del búfer en el servicio overlayd que podría permitir a un atacante la denegación del servicio o la ejecución remota de código.

**Solución:**

- Actualizar a las versiones:
  - 15.1R7-S9;
  - 17.3R3-S11;
  - 17.4R2-S13 y 17.4R3-S4;
  - 18.1R3-S12;
  - 18.2R2-S8 y 18.2R3-S7;
  - 18.3R3-S4;
  - 18.4R1-S8, 18.4R2-S7 y 18.4R3-S7;
  - 19.1R2-S2 y 19.1R3-S4;
  - 19.2R1-S6 y 19.2R3-S2;
  - 19.3R3-S1;
  - 19.4R2-S4 y 19.4R3-S1;
  - 20.1R2-S1 y 20.1R3;
  - 20.2R2, 20.2R2-S1 y 20.2R3;
  - 20.3R1-S1.

**Detalle:**

Una validación incorrecta del tamaño del búfer en el servicio overlayd, de Juniper Networks Junos OS, podría permitir a un atacante remoto, no autenticado, enviar paquetes especialmente diseñados al dispositivo, desencadenando una condición de denegación de servicio (DoS) parcial o conducir a la ejecución remota de código. Se ha asignado el identificador CVE-2021-0254 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Ejecución remota de código en Pulse Connect Secure

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

Pulse Connect Secure, versión 9.0R3 y superior.

**Descripción:**

Se ha descubierto una vulnerabilidad en Pulse Connect Secure (PCS) que podría permitir a un atacante, no autenticado, la ejecución remota de archivos arbitrarios en la puerta de enlace de Pulse Connect Secure. Esta vulnerabilidad supone un riesgo importante y está siendo explotada de forma activa.

**Solución:**

Actualizar a Pulse Connect Secure, versión 9.1R.11.4 cuando esté disponible.

Mientras tanto, Pulse Secure recomienda importar el archivo Workaround-2104.xml, para desactivar los dos conjuntos de características afectadas en las instancias existentes de PCS: Windows File Share Browser y Pulse Secure Collaboration.

**Detalle:**

Una vulnerabilidad expuesta por las funciones de Windows File Share Browser y Pulse Secure Collaboration de Pulse Connect Secure podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario en un sistema de puerta de enlace vulnerable de Pulse Connect Secure. Se ha asignado el identificador CVE-2021-22893 para esta vulnerabilidad.

**Etiquetas:** 0day, Vulnerabilidad

---

# Múltiples vulnerabilidades 0day en SonicWall Email Security

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- Email Security (ES), versiones 10.0.1, 10.0.2, 10.0.3 y 10.0.4 hasta la actual;
- Hosted Email Security (HES), versiones 10.0.1, 10.0.2, 10.0.3 y 10.0.4 hasta la actual.

Las versiones 7.0.0-9.2.2 de SonicWall Email Security también se ven afectadas por estas vulnerabilidades. Sin embargo, estas versiones han llegado al final de su vida útil (EOL) y ya no reciben soporte.

**Descripción:**

FireEye Mandiant Managed Defense ha detectado 3 vulnerabilidades 0day, 1 con severidad crítica y las 2 restantes medias, en SonicWall Email Security (ES) que están siendo explotadas de manera activa para para obtener acceso administrativo y realizar ejecución de código, por lo que es imperativo que las organizaciones que utilizan dispositivos de *hardware*, dispositivos virtuales o instalaciones de *software* de SonicWall Email Security en Microsoft Windows Server actualicen inmediatamente a la respectiva versión que las corrige.

**Solución:**

Actualizar a:

- Email Security 10.0.9.6173 (Windows);
- Email Security 10.0.9.6177 (Hardware y ESXi Virtual Appliance);
- Hosted Email Security 10.0.9.6173 (parcheado automáticamente).

**Detalle:**

- La aplicación SonicWall Email Security contiene un panel de control de autenticación para proporcionar capacidades de administración. Debido a esta vulnerabilidad, un atacante con un documento XML, especialmente diseñado, podría realizar peticiones HTTP a la aplicación y crear una cuenta *role.ouadmin* que podría ser utilizada para autenticarse en la aplicación como administrador. Se ha asignado el identificador CVE-2021-20021 para esta vulnerabilidad crítica.
- La falta de validación en los archivos ZIP subidos a la interfaz web del usuario podría permitir a un atacante subir archivos maliciosos con código ejecutable y *webshells* en ubicaciones arbitrarias. Se ha asignado el identificador CVE-2021-20022 para esta vulnerabilidad.
- Una vulnerabilidad en la autenticación en el *branding* integrado en el panel administrativo podría permitir a un atacante recuperar archivos arbitrarios del *host* enviando peticiones HTTP, especialmente diseñadas, a un recurso concreto. Se ha asignado el identificador CVE-2021-20023 para esta vulnerabilidad.

**Etiquetas:** 0day, Actualización, Comunicaciones, Microsoft, Virtualización, Vulnerabilidad

---

# Vulnerabilidad XSS en TIBCO Administrator

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

Versiones 5.11.0, 5.11.1, 5.10.2 y anteriores de los productos:

- TIBCO Administrator - Enterprise Edition;
- TIBCO Administrator - Enterprise Edition Distribution para TIBCO Silver Fabric;
- TIBCO Administrator - Enterprise Edition para z/Linux;
- TIBCO Runtime Agent;
- TIBCO Runtime Agent para z/Linux;

El componente administration GUI.

**Descripción:**

TIBCO ha notificado una vulnerabilidad crítica, de tipo XSS almacenado, cuya explotación podría permitir que un atacante obtuviese acceso administrativo completo al sistema afectado.

**Solución:**

Actualizar los productos afectados a las versiones 5.10.3, 5.11.2 o superiores, según corresponda a la versión afectada.

**Detalle:**

En los sistemas basados en Unix, existe una vulnerabilidad que podría permitir a un atacante, no autentificado, realizar ingeniería social a un usuario legítimo con acceso a la red para ejecutar un ataque, de tipo XSS almacenado, dirigido al sistema afectado. Se ha asignado el identificador CVE-2021-28827 para esta vulnerabilidad.

**Etiquetas:** Actualización, Linux, Vulnerabilidad

---

# Múltiples vulnerabilidades en ClearPass de Aruba

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- ClearPass 6.9.x, todas las versiones anteriores a la 6.9.5;
- ClearPass 6.8.x, todas las versiones anteriores a la 6.8.9;
- ClearPass 6.7.x, todas las versiones anteriores a la 6.7.14 y 6.7.14-HF1.

**Descripción:**

Varios investigadores han notificado 10 vulnerabilidades, 1 de severidad crítica y 9 de severidad alta, que podrían permitir a un atacante remoto y no autenticado ejecutar código arbitrario, causar un estado de denegación de servicio, acceder a información confidencial o robo de credenciales respectivamente.

**Solución:**

Actualizar:

- ClearPass 6.9.x a la versión 6.9.5 u otra superior;
- ClearPass 6.8.x a la versión 6.8.9 u otra superior;
- ClearPass 6.7.x a la versión 6.7.14 y 6.7.14-HF1 u otra superior respectivamente.

**Detalle:**

Una vulnerabilidad de tipo SSRF (Server Side Request Forgery) en la interfaz web de administración de ClearPass podría permitir a un atacante remoto y no autenticado ejecutar código arbitrario en el host de ClearPass. Se ha asignado el identificador CVE-2021-29145 para esta vulnerabilidad de severidad crítica.

Para el resto de vulnerabilidades se han asignado los identificadores CVE-2021-29139, CVE-2021-29142, CVE-2021-29146, CVE-2021-29140, CVE-2020-7123, CVE-2021-29138, CVE-2020-29147, CVE-2021-29141 y CVE-2021-29144.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

---

# Actualizaciones críticas en Oracle (abril 2021)

**Fecha de publicación:** 21/04/2021

**Importancia:** Crítica

**Recursos afectados:**

- Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite, versiones 3.5 y 3.6;
- Agile Product Lifecycle Management Integration Pack for SAP: Design to Release, versiones 3.5 y 3.6;
- Enterprise Manager Base Platform, versión 13.4.0.0;
- Enterprise Manager for Fusion Middleware, versiones 12.2.1.4 y 13.4.0.0;
- Enterprise Manager for Virtualization, versión 13.4.0.0;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- FMW Platform, versiones 12.2.1.3.0 y 12.2.1.4.0;
- Hyperion Analytic Provider Services, versiones 11.1.2.4 y 12.2.1.4;
- Hyperion Financial Management, versión 11.1.2.4;
- Instantis EnterpriseTrack, versiones 17.1, 17.2 y 17.3;
- JD Edwards EnterpriseOne Orchestrator, todas las versiones anteriores a la 9.2.5.3;
- JD Edwards EnterpriseOne Tools, todas las versiones anteriores a la 9.2.4.0 y 9.2.5.3;
- JD Edwards World Security, versión A9.4;
- MySQL Cluster, versión 8.0.23 y anteriores;
- MySQL Enterprise Monitor, versión 8.0.23 y anteriores;
- MySQL Server, versión 5.7.33 y anteriores, y versión 8.0.23 y anteriores;
- MySQL Workbench, versión 8.0.23 y anteriores;
- Oracle Advanced Supply Chain Planning, versiones 12.1 y 12.2;
- Oracle Agile PLM, versiones 9.3.3, 9.3.5 y 9.3.6;
- Oracle API Gateway, versión 11.1.2.4.0;
- Oracle Application Express, todas las versiones anteriores a la 20.2;
- Oracle Application Testing Suite, versión 13.3.01;
- Oracle BAM, versiones 11.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Banking Platform, versiones 2.4.0, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0 y 2.10.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Cloud Infrastructure Storage Gateway, todas las versiones anteriores a la 1.4;
- Oracle Coherence, versiones 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0;
- Oracle Commerce Guided Search, versiones 11.3.0, 11.3.1 y 11.3.2;
- Oracle Commerce Merchandising, versiones 0, 11.0.0, 11.1, 11.2.0, 11.3.0, 11.3.1 y 11.3.2;
- Oracle Communications Application Session Controller, versión 3.9m0p3;
- Oracle Communications Calendar Server, versión 8.0;
- Oracle Communications Contacts Server, versión 8.0;
- Oracle Communications Converged Application Server ? Service Controller, versión 6.2;
- Oracle Communications Design Studio, versión 7.4.2;
- Oracle Communications Interactive Session Recorder, versiones 6.3 y 6.4;
- Oracle Communications Messaging Server, versiones 8.0.2, 8.1 y 8.1.0;
- Oracle Communications MetaSolv Solution, versiones 6.3.0 y 6.3.1;
- Oracle Communications Performance Intelligence Center Software, versiones 10.4.0.2 y 10.4.0.3;
- Oracle Communications Services Gatekeeper, versiones 6.0, 6.1 y 7.0;
- Oracle Communications Session Border Controller, versiones Cz8.2, Cz8.3 y Cz8.4;
- Oracle Communications Session Router, versiones Cz8.2, Cz8.3 y Cz8.4;
- Oracle Communications Subscriber-Aware Load Balancer, versiones Cz8.2, Cz8.3 y Cz8.4;
- Oracle Communications Unified Inventory Management, versiones 7.3.4, 7.3.5, 7.4.0 y 7.4.1;
- Oracle Communications Unified Session Manager, versión SCz8.2.5;
- Oracle Database Server, versiones 12.1.0.2, 12.2.0.1, 18c y 19c;
- Oracle E-Business Suite, versiones de la 12.1.1 a la 12.1.3 y de la 12.2.3 a la 12.2.10;
- Oracle Endeca Information Discovery Studio, versión 3.2.0.0;
- Oracle Enterprise Communications Broker, versiones PCZ3.1, PCZ3.2 y PCZ3.3;
- Oracle Enterprise Repository, versión 11.1.1.7.0;
- Oracle Enterprise Session Border Controller, versiones Cz8.2, Cz8.3 y Cz8.4;
- Oracle Financial Services Analytical Applications Infrastructure, versiones de la 8.0.6 a la 8.1.0;
- Oracle FLEXCUBE Direct Banking, versiones 12.0.2 y 12.0.3;
- Oracle FLEXCUBE Private Banking, versiones 12.0.0 y 12.1.0;
- Oracle Fusion Middleware, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Fusion Middleware MapViewer, versión 12.2.1.4.0;
- Oracle Global Lifecycle Management OPatch, todas las versiones anteriores a la 12.2.0.1.22;
- Oracle GraalVM Enterprise Edition, versiones 19.3.5, 20.3.1.2 y 21.0.0.2;

- Oracle Graph Server and Client;
- Oracle Health Sciences Empirica Signal, versiones 9.0 y 9.1;
- Oracle Health Sciences Information Manager, versiones de la 3.0.0 a la 3.0.2;
- Oracle Healthcare Foundation, versiones 7.1.5, 7.2.2, 7.3.0, 7.3.1 y 8.0.1;
- Oracle Hospitality Cruise Shipboard Property Management System, versión 20.1.0;
- Oracle Hospitality Inventory Management, versión 9.1.0;
- Oracle Hospitality OPERA 5, versiones 5.5 y 5.6;
- Oracle Hospitality RES 3700, versiones de la 5.7.0 a la 5.7.6;
- Oracle HTTP Server, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Identity Manager Connector, versión 11.1.1.5.0;
- Oracle iLearning, versiones 6.2 y 6.3;
- Oracle Insurance Data Gateway, versión 1.0.2.3;
- Oracle Java SE, versiones 7u291, 8u281, 11.0.10 y 16;
- Oracle Java SE Embedded, versión 8u281;
- Oracle NoSQL Database, todas las versiones anteriores a la 20.3;
- Oracle Outside In Technology, versión 8.5.5;
- Oracle Platform Security for Java, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Rapid Planning, versión 12.1.3;
- Oracle REST Data Services, todas las versiones anteriores a la 20.4.3.50.1904;
- Oracle Retail Advanced Inventory Planning, versión 14.1;
- Oracle Retail Assortment Planning, versión 16.0.3;
- Oracle Retail Back Office, versión 14.1;
- Oracle Retail Category Management Planning & Optimization, versión 16.0.3;
- Oracle Retail Central Office, versión 14.1;
- Oracle Retail EFTLink, versiones 15.0.2, 16.0.3, 17.0.2, 18.0.1, 19.0.1 y 20.0.0;
- Oracle Retail Insights Cloud Service Suite, versión 19.0;
- Oracle Retail Item Planning, versión 16.0.3;
- Oracle Retail Macro Space Optimization, versión 16.0.3;
- Oracle Retail Merchandise Financial Planning, versión 16.0.3;
- Oracle Retail Merchandising System, versión 16.0.3;
- Oracle Retail Point-of-Service, versión 14.1;
- Oracle Retail Predictive Application Server, versiones 14.1, 15.0 y 16.0;
- Oracle Retail Regular Price Optimization, versión 16.0.3;
- Oracle Retail Replenishment Optimization, versión 16.0.3;
- Oracle Retail Returns Management, versión 14.1;
- Oracle Retail Sales Audit, versión 14.0;
- Oracle Retail Size Profile Optimization, versión 16.0.3;
- Oracle Retail Store Inventory Management, versiones 14.1.3.10, 15.0.3.5 y 16.0.3.5;
- Oracle Retail Xstore Point of Service, versiones 15.0.4, 16.0.6, 17.0.4, 18.0.3 y 19.0.2;
- Oracle SD-WAN Aware, versión 8.2;
- Oracle SD-WAN Edge, versiones 8.2 y 9.0;
- Oracle Secure Backup;
- Oracle Secure Global Desktop, versión 5.6;
- Oracle Security Service, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Service Bus, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Solaris, versiones 10 y 11;
- Oracle Spatial Studio, todas las versiones anteriores a la 19.1.0 y 20.1.1;
- Oracle SQL Developer, todas las versiones anteriores a la 20.4.1.407.6 ;
- Oracle Storage Cloud Software Appliance, todas las versiones anteriores a la 16.3.1.4.2;
- Oracle TimesTen In-Memory Database;
- Oracle Utilities Framework, versiones 4.2.0.2.0, 4.2.0.3.0, de la 4.3.0.1.0 a la 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0 y 4.4.0.3.0;
- Oracle VM VirtualBox, todas las versiones anteriores a la 6.1.20;
- Oracle WebCenter Portal, versiones 12.2.1.3.0 y 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 y 14.1.1.0.0;
- Oracle WebLogic Server Proxy Plug-In, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle ZFS Storage Appliance Kit, versión 8.8;
- OSS Support Tools, todas las versiones anteriores a la 2.12.41;
- PeopleSoft Enterprise CS Campus Community, versión 9.2 ;
- PeopleSoft Enterprise FIN Common Application Objects, versión 9.2;
- PeopleSoft Enterprise FIN Expenses, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57 y 8.58;
- PeopleSoft Enterprise PT PeopleTools, versiones 8.56, 8.57 y 8.58;
- PeopleSoft Enterprise SCM eProcurement, versión 9.2;
- PeopleSoft Enterprise SCM Purchasing, versión 9.2;
- Primavera Gateway, versiones de la 17.12.0 a la 17.12.10;
- Primavera Unifier, versiones 16.1, 16.2, de la 17.7 a la 17.12, 18.8, 19.12 y 20.12;
- Siebel Applications, versión 21.2 y anteriores.

**Descripción:**

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades que afectan a múltiples productos.

**Solución:**

Aplicar los parches correspondientes según los productos afectados. La información para descargar las actualizaciones puede obtenerse del boletín de seguridad publicado por Oracle.

**Detalle:**

Esta actualización resuelve un total de 390 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

# Vulnerabilidad en el core de Drupal

**Fecha de publicación:** 22/04/2021

**Importancia:** Crítica

**Recursos afectados:**

Versiones anteriores a:

- 9.1.17;
- 9.0.12;
- 8.9.14;
- 7.80.

**Descripción:**

Se ha publicado una vulnerabilidad de severidad crítica en el core de Drupal que podría permitir realizar ataques de cross-site scripting.

**Solución:**

Actualizar a las versiones 9.1.7, 9.0.12, 8.9.14, 7.80.

Las versiones de Drupal 8, anteriores a la 8.9.x, están al final de su vida útil y ya no reciben cobertura de seguridad.

**Detalle:**

La API de sanitización del core de Drupal no filtra adecuadamente el cross-site scripting en algunas circunstancias.

**Etiquetas:** Actualización, CMS, Vulnerabilidad

---

# Omisión de autenticación en FortiWAN

**Fecha de publicación:** 28/04/2021

**Importancia:** Crítica

**Recursos afectados:**

FortiWAN, versiones 4.5.7 y anteriores.

**Descripción:**

Una vulnerabilidad de limitación incorrecta de nombre de ruta relativa a un directorio restringido (Relative Path Traversal) podría permitir a un atacante remoto, no autenticado, eliminar archivos en el sistema.

**Solución:**

- Actualizar a la próxima versión de FortiWAN 4.5.8 o superior.
- Actualizar a la versión 5.1.1 o superior de FortiWAN.

Como medida de mitigación, en lugar de permitir el acceso administrativo desde cualquier fuente, restríngalo a los hosts internos de confianza.

**Detalle:**

Una vulnerabilidad de limitación incorrecta de nombre de ruta relativa a un directorio restringido (Relative Path Traversal) en FortiWAN podría permitir a un atacante remoto, no autenticado, eliminar archivos en el sistema enviando una solicitud POST especialmente diseñada. En particular, la eliminación de archivos de configuración específicos restablecerá la contraseña de administrador a su valor predeterminado. Se ha asignado el identificador CVE-2021-26102 para esta vulnerabilidad.

**Etiquetas:** Actualización, Comunicaciones, Virtualización, Vulnerabilidad

---

# Control inadecuado de los recursos en Citrix ShareFile

**Fecha de publicación:** 28/04/2021

**Importancia:** Crítica

**Recursos afectados:**

Citrix ShareFile controlador de zonas de almacenamiento, versiones:

- 5.7 anteriores a 5.7.3;
- 5.8 anteriores a 5.8.3;
- 5.9 anteriores a 5.9.3;
- 5.10 anteriores a 5.10.1;

- 5.11 anteriores a 5.11.18.

**Descripción:**

Citrix ha identificado una vulnerabilidad, de severidad crítica, de control inadecuado de recursos que afecta a ShareFile.

**Solución:**

Actualizar Citrix ShareFile a las siguientes versiones:

- 5.7.3 y posteriores de 5.7;
- 5.8.3 y posteriores de 5.8;
- 5.9.3 y posteriores de 5.9;
- 5.10.1 y posteriores de 5.10;
- 5.11.18 y posteriores de 5.11.

**Detalle:**

Se ha identificado una vulnerabilidad en el controlador de zonas de almacenamiento de Citrix ShareFile que podría permitir a un atacante remoto, no autenticado, comprometer el controlador de zonas de almacenamiento, siempre y cuando previamente se tenga acceso a la red del controlador de zonas de almacenamiento. Se ha asignado el identificador CVE-2021-22891 para esta vulnerabilidad.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

---

# Omisión de autenticación en HPE Edgeline Infrastructure Manager

**Fecha de publicación:** 30/04/2021

**Importancia:** Crítica

**Recursos afectados:**

HPE Edgeline Infrastructure Manager, versiones anteriores a 1.22.

**Descripción:**

Tenable Research ha notificado a HPE sobre una vulnerabilidad crítica, de omisión de autenticación explotable de forma remota, que afecta a su producto Edgeline Infrastructure Manager.

**Solución:**

Actualizar HPE Edgeline Infrastructure a la versión 1.22 o posteriores desde el centro de soporte del fabricante.

**Detalle:**

Un atacante remoto podría aprovechar esta vulnerabilidad para eludir la autenticación remota, lo que podría ocasionar una ejecución de comandos arbitrarios, obtención de acceso privilegiado, provocar una condición de denegación de servicio (DoS) y cambiar la configuración del dispositivo afectado. Se ha asignado el identificador CVE-2021-29203 para esta vulnerabilidad.

**Etiquetas:** Actualización, HP, Vulnerabilidad