Boletín de marzo de 2021

Avisos Técnicos

Actualización fuera de ciclo de Microsoft Exchange Server

Fecha de publicación: 03/03/2021

Importancia: Crítica

Recursos afectados:

- Microsoft Exchange Server 2013,
- Microsoft Exchange Server 2016,
- Microsoft Exchange Server 2019.

Descripción:

Microsoft ha publicado actualizaciones de seguridad fuera del ciclo mensual habitual, para solucionar varias vulnerabilidades que afectan a Microsoft Exchange Server. Un atacante remoto podría aprovechar varias de estas vulnerabilidades de ejecución remota de código para tomar el control de un sistema afectado, o aprovechar otra de las vulnerabilidades para obtener acceso a información confidencial.

La empresa ha confirmado que estas vulnerabilidades se están explotando de forma activa actualmente.

Solución:

Microsoft ha publicado las siguientes actualizaciones de seguridad:

- Exchange Server 2010 (RU 31 para Service Pack 3: esta actualización es con fines de defensa en profundidad),
- Exchange Server 2013 (CU 23),
- Exchange Server 2016 (CU 19, CU 18),
- Exchange Server 2019 (CU 8, CU 7).

Además, recomienda instalar estas actualizaciones de manera inmediata.

Igualmente, ha compartido los indicadores de compromiso (IOC) para poder verificar si sus sistemas se han visto afectados por este ataque.

Detalle:

Microsoft ha informado de la existencia de varias vulnerabilidades, que en su conjunto podrían comprometer un equipo con Microsoft Exchange Server. Los identificadores de estas vulnerabilidades son: CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, y CVE-2021-26855.

El vector inicial del ataque se establece a través de una conexión no confiable con el puerto 443 del servidor Exchange, pero el bloqueo de estas conexiones solo protege de una parte inicial del ataque. No obstante, otros vectores pueden activarse si un atacante ya tiene acceso.

Microsoft ha confirmado que estas vulnerabilidades se están explotando de forma activa actualmente por un grupo identificado como HAFNIUM.

Etiquetas: 0day, Actualización, Microsoft, Vulnerabilidad, Windows

Múltiples vulnerabilidades en GRUB2

Fecha de publicación: 03/03/2021

Importancia: Alta

Recursos afectados:

Todos los sistemas que hagan uso de GRUB2.

Descripción:

Se han reportado varios fallos de seguridad en GRUB2 que podrían permitir a un atacante cargar tablas ACPI especialmente diseñadas, ejecutar código arbitrario, eludir las protecciones de Secure Boot, arrancar un kernel especialmente diseñado o corromper la memoria.

Solución:

Se han publicado 117 parches que solucionan estas vulnerabilidades. Además, se está trabajando en un esquema de revocación basado en el número de generación denominado UEFI Secure Boot Advanced Targeting (SBAT) que requerirá una liberación de UEFI dbx y renunciar a todos los artefactos (shim, GRUB, kernel, etc.) necesarios para arrancar el sistema, así como la creación de una lista de revocación UEFI (dbx). Los diferentes fabricantes y distribuciones publicarán las respectivas instrucciones de actualización.

Puede consultar la sección de Referencias para obtener más información sobre las actualizaciones de diferentes fabricantes.

Detalle:

- El comando acpi permite al usuario privilegiado cargar tablas ACPI especialmente diseñadas, cuando el arranque seguro está activado. Se ha asignado el identificador CVE-2020-14372 para esta vulnerabilidad.
- Una vulnerabilidad de uso de memoria previamente liberada en el comando *rmmod* podría permitir a un atacante ejecutar código arbitrario y eludir las protecciones de Secure Boot. Se ha asignado el identificador CVE-2020-25632 para esta vulnerabilidad.
- Una escritura fuera de límites en grub_usb_device_initialize() podría permitir a un atacante la ejecución de código arbitrario, permitiendo eludir los mecanismos de protección de Secure Boot. Se ha asignado el identificador CVE-2020-25647 para esta vulnerabilidad.
- Un desbordamiendo de búfer basado en pila (stack), en grub_parser_split_cmdline, podría permitir a un atacante eludir los mecanismos de protección de Secure Boot. Se ha asignado el identificador CVE-2020-27749 para esta vulnerabilidad.
- El comando cutmem permite a un usuario con privilegios borrar regiones de memoria cuando Secure Boot está activado. Se ha asignado el identificador CVE-2020-27779 para esta vulnerabilidad.
- Un fallo que afecta a upstream y a las distribuciones que utilizan el verificador shim_lock podría permitir el arranque de cualquier kernel especialmente diseñado, sin validación de firma, al reintroducir la vulnerabilidad CVE-2020-15705 en GRUB 2.05. Se ha asignado el identificador CVE-2021-3418 para esta vulnerabilidad.
- El analizador de opciones de GRUB2 podría permitir a un atacante el desbordamiento de búfer basado en memoria dinámica (heap). Se ha asignado el identificador CVE-2021-20225 para esta vulnerabilidad.
- El desbordamiento de búfer basado en memoria dinámica (*heap*) debido a un cálculo erróneo del espacio necesario para las citas (*quotes*) podría permitir a un atacante corromper la memoria. Se ha asignado el identificador CVE-2021-20233 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Microsoft, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.25

Fecha de publicación: 03/03/2021

Importancia: Media

Recursos afectados:

Joomla! CMS, versiones:

- desde la 3.2.0, hasta la 3.9.24;
- desde la 3.0.0, hasta la 3.9.24;
- desde la 2.5.0, hasta la 3.9.24;
- desde la 1.6.0, hasta la 3.9.24.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 10 vulnerabilidades que afectan a su núcleo, de los tipos aleatoriedad insegura, XSS (*Cross Site Scripting*), validación de entrada incorrecta, violación ACL (*Access Control List*) y limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*).

Solución:

Actualizar a la versión 3.9.25.

Detalle:

- Uso de la función insegura *rand()* dentro del proceso de generación de 2FA (autenticación de dos factores). Se ha asignado el identificador CVE-2021-23126 para esta vulnerabilidad.
- Uso de una longitud insuficiente para el proceso 2FA según el RFC 4226 de 10 bytes frente a 20 bytes. Se ha asignado el identificador CVE-2021-23127 para esta vulnerabilidad.
- La implementación de *randval* en el núcleo de FOF (*FOFEncryptRandval*), a pesar de no ser utilizada, empleaba una implementación potencialmente insegura que ha sido reemplazada por una llamada a *random_bytes()* y su *backport* que se envía dentro de *random_compat*. Se ha asignado el identificador CVE-2021-23128 para esta vulnerabilidad.
- La falta de filtrado de los mensajes mostrados a los usuarios podrían dar lugar a una vulnerabilidad de XSS. Se ha

asignado el identificador CVE-2021-23129 para esta vulnerabilidad.
- La falta de filtrado de los campos de *feed* podría dar lugar a una vulnerabilidad de XSS. Se ha asignado el identificador CVE-2021-23130 para esta vulnerabilidad.
- Falta la validación de entradas en el gestor de plantillas. Se ha asignado el identificador CVE-2021-23131 para esta vulnerabilidad.
- El componente *com_media* podría permitir rutas que no están destinadas a la carga de imágenes. Se ha asignado el identificador CVE-2021-23132 para esta vulnerabilidad.
- Las comprobaciones incorrectas de ACL podrían permitir el cambio no autorizado de la categoría de un artículo. Se ha asignado el identificador CVE-2021-26027 para esta vulnerabilidad.
- La extracción de un paquete zip, específicamente diseñado, podría modificar archivos fuera de la ruta prevista. Se ha asignado el identificador CVE-2021-26028 para esta vulnerabilidad.
- Un filtrado inadecuado del contenido de los formularios podría permitir sobrescribir el campo *author*. Los componentes principales afectados son *com_fields*, *com_categories*, *com_banners*, *com_contact*, *com_newsfeeds* y *com_tags*. Se ha asignado el identificador CVE-2021-26029 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Actualización de seguridad de SAP de marzo de 2021

Fecha de publicación: 10/03/2021

Importancia: Crítica

Recursos afectados:

- SAP Solution Manager (User Experience Monitoring), versión 7.2;
- SAP Business Client, versión 6.5;
- SAP Manufacturing Integration e Intelligence, versiones 15.1, 15.2, 15.3 y 15.4;
- SAP NetWeaver AS JAVA (MigrationService), versiones 7.10, 7.11, 7.30, 7.31, 7.40 y 7.50;
- SAP HANA, versión 2.0;
- SAP Enterprise Financial Services (Bank Customer Accounts), versiones 101, 102, 103, 104, 105, 600, 603, 604, 605, 606, 616, 617, 618 y 800;
- SAP NetWeaver Knowledge Management, versiones 7.01, 7.02, 7.30,7.31, 7.40 y 7.50;
- SAP Payment Engine, versión 500;
- SAP BusinessObjects Business Intelligence Platform (Web Services), versiones 410, 420 y 430;
- 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 3D Visual Enterprise Viewer, versión 9;
- SAP ERP, versiones 600, 602, 603, 604, 605, 606, 616, 617 y 618;
- SAP S/4 HANA, versiones 100, 101, 102, 103 y 104;

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 9 notas de seguridad y 4 actualizaciones de notas anteriores, siendo 4 de severidad crítica, 1 alta y 8 medias.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 2 vulnerabilidades de falta de comprobación de autenticación,
- 1 vulnerabilidad de inyección de código,
- 10 vulnerabilidades de validación incorrecta de entrada,
- 4 vulnerabilidades de falta de comprobación de autorización,
- 1 vulnerabilidad de SSRF (*Server Side Request Forgery*),
- 4 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- SAP Manufacturing Intelligence and Integrations (SAP MII): se corrige una vulnerabilidad de inyección de código muy crítica en la que un atacante puede interceptar una solicitud al servidor, inyectar código JSP malicioso en la solicitud y reenviarlo al servidor. Se ha asignado el identificador CVE-2021-21480 para esta vulnerabilidad.
- SAP NetWeaver AS JAVA (MigrationService): se corrige la verificación de autorización que podría permitir a un atacante no autorizado obtener privilegios administrativos. Esto podría resultar en un compromiso total de la confidencialidad, integridad y disponibilidad del sistema. Se ha asignado el identificador CVE-2021-21481 para esta vulnerabilidad.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualizaciones de seguridad de Microsoft de marzo de 2021

Fecha de publicación: 10/03/2021

Importancia: Crítica

Recursos afectados:

- Application Virtualization;
- Azure;
- Azure DevOps;
- Azure Sphere;
- Internet Explorer;
- Microsoft ActiveX;
- Microsoft Exchange Server;
- Microsoft Edge (Chromium-based);
- Microsoft Graphics Component;
- Microsoft Office;
- Microsoft Office Excel;
- Microsoft Office PowerPoint;
- Microsoft Office SharePoint;
- Microsoft Office Visio;
- Microsoft Windows Codecs Library;
- Power BI;
- Role: DNS Server;
- Role: Hyper-V;
- Visual Studio;
- Visual Studio Code;
- Windows Admin Center;
- Windows Container Execution Agent;
- Windows DirectX;
- Windows Error Reporting;
- Windows Event Tracing;
- Windows Extensible Firmware Interface;
- Windows Folder Redirection;
- Windows Installer;
- Windows Media;
- Windows Overlay Filter;
- Windows Print Spooler Components;
- Windows Projected File System Filter Driver;
- Windows Registry;
- Windows Remote Access API;
- Windows Storage Spaces Controller;
- Windows Update Assistant;
- Windows Update Stack;
- Windows UPnP Device Host;
- Windows User Profile Service;
- Windows WalletService;
- Windows Win32K.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de marzo, consta de 89 vulnerabilidades, clasificadas 14 como críticas y 75 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:

- denegación de servicio;
- escalada de privilegios;
- divulgación de información;
- ejecución remota de código;
- elusión de las medidas de seguridad;
- suplantación de identidad (*spoofing*).

Microsoft también ha corregido hoy otras dos vulnerabilidades 0day con identificadores CVE-2021-26411 y CVE-2021-27077.

Etiquetas: 0day, Actualización, Microsoft, Navegador, Privacidad, Virtualización, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en varios productos de F5

Fecha de publicación: 11/03/2021

Importancia: Crítica

Recursos afectados:

- BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO),

versiones:
    - 16.0.0 - 16.0.1;
    - 15.1.0 - 15.1.2;
    - 14.1.0 - 14.1.3;
    - 13.1.0 - 13.1.3;
    - 12.1.0 - 12.1.5;
    - 11.6.1 - 11.6.5.
- BIG-IQ Centralized Management, versiones:
    - 7.1.0 y 7.0.0;
    - 6.0.0 - 6.1.0.

Descripción:

Se han identificado 4 vulnerabilidades en varios productos de F5, todas con severidad crítica, de tipo desbordamiento de búfer y ejecución remota de comandos.

Solución:

Actualizar los productos afectados a las siguientes versiones:

- BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO):
    - 16.0.1.1;
    - 15.1.2.1;
    - 14.1.4;
    - 13.1.3.6;
    - 12.1.5.3;
    - 11.6.5.3.
- BIG-IQ Centralized Management:
    - 8.0.0;
    - 7.1.0.3 o 7.0.0.2.

Detalle:

- Un atacante, con acceso a los servidores web del *backend*, podría enviar una respuesta HTTP, especialmente diseñada, al servidor virtual Advanced WAF/ASM y generar un desbordamiento de búfer, lo que posibilitaría ataques de denegación de servicio (DoS) o de ejecución remota de código (RCE). Se ha asignado el identificador CVE-2021-22992 para esta vulnerabilidad.
- Un atacante no autenticado, con acceso de red de la interfaz iControl REST, podría aprovechar una vulnerabilidad de tipo RCE para ejecutar comandos arbitrarios del sistema, crear/modificar archivos y deshabilitar servicios. Se ha asignado el identificador CVE-2021-22986 para esta vulnerabilidad.
- Un atacante autenticado, con acceso de red a Traffic Management User Interface (TMUI) y ejecutando en modo *Appliance*, podría aprovechar una vulnerabilidad de tipo RCE en páginas no publicadas para ejecutar comandos arbitrarios del sistema, crear/modificar archivos y deshabilitar servicios. Se ha asignado el identificador CVE-2021-22987 para esta vulnerabilidad.
- Algunas solicitudes a un servidor virtual podrían ser gestionadas incorrectamente durante el proceso de normalización de la URI en Traffic Management Microkernel (TMM), lo que podría desencadenar un desbordamiento de búfer, dando lugar a un ataque DoS. En ciertas situaciones, podría permitir eludir el control de acceso basado en URL o realizar un RCE. Se ha asignado el identificador CVE-2021-22991 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 15/03/2021

Importancia: Crítica

Recursos afectados:

Las versiones de Moodle que se ven afectadas son las siguientes:

- de la 3.10 a la 3.10.1;
- de la 3.9 a la 3.9.4;
- de la 3.8 a la 3.8.7;
- de la 3.5 a la 3.5.16;
- versiones anteriores no soportadas.

Descripción:

Se han publicado 7 vulnerabilidades en Moodle, 2 de severidad crítica y 5 de severidad baja, que podrían permitir a un atacante realizar ataques de tipo XSS almacenado o SSRF ciego.

Solución:

Aplicar las siguientes actualizaciones, en función de la versión afectada:

- 3.10.2;
- 3.9.5;
- 3.8.8;
- 3.5.17.

Detalle:

- Una validación o filtrado insuficientes en el campo para introducir el ID del usuario podría permitir a un usuario malintencionado realizar un ataque de tipo XSS almacenado (*stored*). Se ha asignado el identificador CVE-2021-20279

para esta vulnerabilidad crítica.
- Un filtrado insuficiente en las respuestas de feedback podría permitir a un usuario malintencionado realizar un ataque de tipo XSS almacenado o SSRF ciego (*blind*). Se ha asignado el identificador CVE-2021-20280 para esta vulnerabilidad crítica.

Para las vulnerabilidades de severidad baja, se han asignado los identificadores CVE-2020-11022, CVE-2020-11023, CVE-2021-20283, CVE-2021-20282 y CVE-2021-20281.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en IBM Security Privileged Identity Manager

Fecha de publicación: 16/03/2021

Importancia: Crítica

Recursos afectados:

IBM Security Privileged Identity Manager (ISPIM), versiones:

- 2.1.1;
- 2.1.0;
- 2.0.2.

Descripción:

El fabricante ha publicado 2 vulnerabilidades, ambas de severidad crítica y de tipo ejecución remota de código, que afectan a varias versiones de IBM Security Privileged Identity Manager.

Solución:

Actualizar ISPIM a las siguientes versiones:

- 2.1.1-ISS-ISPIM-VA-FP0006;
- 2.1.0-ISS-ISPIM-VA-FP0013;
- 2.0.2-ISS-ISPIM-VA-FP0013.

Detalle:

- IBM WebSphere Application Server, versiones 8.5 y 9.0, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema con una secuencia, especialmente diseñada, de objetos serializados. Se ha asignado el identificador CVE-2020-4450 para esta vulnerabilidad.
- IBM WebSphere Application Server Network Deployment, versiones 7.0, 8.0, 8.5, y 9.0, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema con una secuencia, especialmente diseñada, de objetos serializados desde fuentes no confiables. Se ha asignado el identificador CVE-2020-4448 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Ejecución remota de código en SimpliVity OmniStack y en OmniCube de HPE

Fecha de publicación: 16/03/2021

Importancia: Crítica

Recursos afectados:

- HPE SimpliVity 2600 Gen10, depende de la versión ESXi, consulte la guía de interoperabilidad;
- HPE SimpliVity 380 Gen10, depende de la versión ESXi, consulte la guía de interoperabilidad;
- HPE SimpliVity 380 Gen10 G, depende de la versión ESXi, consulte la guía de interoperabilidad;
- HPE SimpliVity 380 Gen10 H, depende de la versión ESXi, consulte la guía de interoperabilidad;
- HPE SimpliVity 380 Gen9, depende de la versión ESXi, consulte la guía de interoperabilidad;
- HPE SimpliVity 325, depende de la versión ESXi, consulte la guía de interoperabilidad;
- SimpliVity OmniStack for Cisco, HPE OmniStack 3.7.10 U1 o anterior;
- SimpliVity OmniStack for Dell, HPE OmniStack 3.7.10 U1 o anterior;
- SimpliVity OmniStack for Lenovo, HPE OmniStack 3.7.10 U1 o anterior;
- SimpliVity OmniCube, HPE OmniStack 3.7.10 U1 o anterior.

Descripción:

Se ha publicado una vulnerabilidad crítica que afecta a varios productos de HPE y que podría permitir a un atacante la ejecución remota de código.

Solución:

- Para ESXi versión 6.5, aplicar ESXi 6.5 EP 23;
- para ESXi versión 6.7, aplicar ESXi 6.7 P04;
- para ESXi versión 7.0, aplicar ESXi 7.0 Update 1b.

Detalle:

Una vulnerabilidad de uso de memoria previamente liberada, presente en los sistemas que se ejecutan en varias versiones del hipervisor ESXi, puede afectar a los sistemas HPE SimpliVity que se ejecutan en cualquiera de las versiones afectadas, y podría permitir a un atacante que resida en la red de gestión y que tenga acceso al puerto 427, en el host ESXi, realizar una ejecución remota de código. Se ha asignado el identificador CVE-2020-3992 para esta vulnerabilidad.

Etiquetas: Actualización, HP, VMware, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de NETGEAR

Fecha de publicación: 16/03/2021

Importancia: Crítica

Recursos afectados:

Los siguientes *switches* que ejecuten cualquier versión de *firmware* anterior a la 2.6.0.48:

- JGS516PE;
- GS116Ev2;
- JGS524PE;
- JGS524Ev2.

Descripción:

NCCgroup ha notificado a NETGEAR 1 vulnerabilidad de severidad crítica, otra de severidad alta y 2 de severidad media, por las que un atacante podría comprometer los equipos.

Solución:

Descargar la versión de firmware más reciente desde la página web de NETGEAR.

Como soluciones alternativas, el fabricante recomienda:

- Sólo administrar el *switch* a través de su interfaz web nativa.
- Habilitar sólo el navegador web como modo de administración y no Plus Utility.
- Posicionar el *switch* detrás de un cortafuegos para no exponerlo directamente a Internet.

Detalle:

- Un atacante podría comprometer el equipo debido a una vulnerabilidad en el control de acceso a nivel de función. Se ha asignado el identificador CVE-2020-26919 para esta vulnerabilidad de severidad crítica.
- Una mala configuración relacionada con la presencia de un servidor TFTP activo de forma predeterminada podría permitir a un atacante remoto comprometer los equipos. Se ha asignado el identificador CVE-2020-35220 para esta vulnerabilidad de severidad alta.

Para las vulnerabilidades de severidad media se han asignado los identificadores CVE-2020-35222 y CVE-35232 respectivamente.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de NETGEAR

Fecha de publicación: 19/03/2021

Importancia: Crítica

Recursos afectados:

- RBW30, ejecutando versiones de *firmware* anteriores a 2.6.2.2;
- RBS40V, ejecutando versiones de *firmware* anteriores a 2.6.2.4;
- RBK852, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBK853, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBK854, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR850, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBS850, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR752, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR753, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR753S, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR754, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBR750, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBS750, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBK752, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBK753, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- RBK753S, ejecutando versiones de *firmware* anteriores a 3.2.17.12;

- RBK754, ejecutando versiones de *firmware* anteriores a 3.2.17.12;
- R6700v3, ejecutando versiones de *firmware* anteriores a 1.0.4.98;
- R6400v2, ejecutando versiones de *firmware* anteriores a 1.0.4.98;
- R7000, ejecutando versiones de *firmware* anteriores a 1.0.11.106;
- R6900P, ejecutando versiones de *firmware* anteriores a 1.3.2.124;
- R7000P, ejecutando versiones de *firmware* anteriores a 1.3.2.124;
- R7900, ejecutando versiones de *firmware* anteriores a 1.0.4.26;
- R7850, ejecutando versiones de *firmware* anteriores a 1.0.5.60;
- R8000, ejecutando versiones de *firmware* anteriores a 1.0.4.58;
- RS400, ejecutando versiones de *firmware* anteriores a 1.5.0.48;
- R6400, ejecutando versiones de *firmware* anteriores a 1.0.1.62;
- R6700, ejecutando versiones de *firmware* anteriores a 1.0.2.16;
- R6900, ejecutando versiones de *firmware* anteriores a 1.0.2.16;
- MK60, 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;
- CBR40, ejecutando versiones de *firmware* anteriores a 2.5.0.10;
- R8000P, ejecutando versiones de *firmware* anteriores a 1.4.1.62;
- R7960P, ejecutando versiones de *firmware* anteriores a 1.4.1.62;
- R7900P, ejecutando versiones de *firmware* anteriores a 1.4.1.62;
- RAX15, ejecutando versiones de *firmware* anteriores a 1.0.1.64;
- RAX20, ejecutando versiones de *firmware* anteriores a 1.0.1.64;
- RAX75, ejecutando versiones de *firmware* anteriores a 1.0.3.102;
- RAX80, ejecutando versiones de *firmware* anteriores a 1.0.3.102;
- RAX200, ejecutando versiones de *firmware* anteriores a 1.0.2.102;
- RAX45, ejecutando versiones de *firmware* anteriores a 1.0.2.64;
- RAX50, ejecutando versiones de *firmware* anteriores a 1.0.2.64;
- EX7500, ejecutando versiones de *firmware* anteriores a 1.0.0.68;
- EAX80, ejecutando versiones de *firmware* anteriores a 1.0.1.62;
- EAX20, ejecutando versiones de *firmware* anteriores a 1.0.0.36;
- RBK842, ejecutando versiones de *firmware* anteriores a 3.2.16.6;
- RBR840, ejecutando versiones de *firmware* anteriores a 3.2.16.6;
- RBS840, ejecutando versiones de *firmware* anteriores a 3.2.16.6;
- 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;
- R6260, ejecutando versiones de *firmware* anteriores a 1.1.0.76;
- R6850, ejecutando versiones de *firmware* anteriores a 1.1.0.76;
- R6350, ejecutando versiones de *firmware* anteriores a 1.1.0.76;
- R6330, ejecutando versiones de *firmware* anteriores a 1.1.0.76;
- D7800, ejecutando versiones de *firmware* anteriores a 1.0.1.58;
- 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;
- RBK40, ejecutando versiones de *firmware* anteriores a 2.6.1.36 / 2.6.1.38;
- RBR40, ejecutando versiones de *firmware* anteriores a 2.6.1.36;
- RBS40, ejecutando versiones de *firmware* anteriores a 2.6.1.38;
- RBK23, ejecutando versiones de *firmware* anteriores a 2.6.1.36 / 2.6.1.38;
- RBR20, ejecutando versiones de *firmware* anteriores a 2.6.1.38;
- RBS20, ejecutando versiones de *firmware* anteriores a 2.6.1.38;
- RBK12, ejecutando versiones de *firmware* anteriores a 2.6.1.44;
- RBK13, ejecutando versiones de *firmware* anteriores a 2.6.1.44;
- RBK14, ejecutando versiones de *firmware* anteriores a 2.6.1.44;
- RBK15, 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;
- R6800, ejecutando versiones de *firmware* anteriores a 1.2.0.72;
- R6900v2, ejecutando versiones de *firmware* anteriores a 1.2.0.72;
- R6700v2, 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;
- 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;
- R7800, ejecutando versiones de *firmware* anteriores a 1.0.2.74;
- R8900, ejecutando versiones de *firmware* anteriores a 1.0.5.24;
- R9000, ejecutando versiones de *firmware* anteriores a 1.0.5.24;
- RAX120, ejecutando versiones de *firmware* anteriores a 1.0.1.136;
- 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;
- XR300, ejecutando versiones de *firmware* anteriores a 1.0.3.50.

Descripción:

Los investigadores *wtbw*, *touhidshaikh* y *talsonor* han reportado 10 vulnerabilidades, todas de severidad crítica, por las que un atacante podría comprometer los equipos afectados.

Solución:

Descargar la versión de *firmware* más reciente desde la página web de soporte de NETGEAR.

Detalle:

Los tipos de vulnerabilidades publicadas, todas ellas críticas, se corresponden con los siguientes:

- divulgación de información sensible,
- omisión de autenticación,
- inyección de comandos después de la autenticación,
- inyección de comandos previa a la autenticación,
- desbordamiento de búfer después de la autenticación.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad en TIBCO API Exchange Gateway

Fecha de publicación: 24/03/2021

Importancia: Crítica

Recursos afectados:

- TIBCO API Exchange Gateway, versión 2.3.3 y anteriores;
- TIBCO API Exchange Gateway Distribution para TIBCO Silver Fabric, versión 2.3.3 y anteriores;
- el componente Config UI también se ve afectado.

Descripción:

TIBCO ha publicado una vulnerabilidad de secuestro de click que podría permitir a un atacante obtener acceso al sistema como administrador.

Solución:

- Actualizar a TIBCO API Exchange Gateway, versión 2.4.0 o superior;
- actualizar a TIBCO API Exchange Gateway Distribution para TIBCO Silver Fabric, versión 2.4.0 o superior.

Detalle:

Una vulnerabilidad de secuestro de click (*clickjacking*) podría permitir a un atacante no autenticado, con acceso a la red, obtener acceso como administrador en el sistema sin intervención de ningún otro usuario. Se ha asignado el identificador CVE-2021-23274 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Cisco Jabber

Fecha de publicación: 25/03/2021

Importancia: Crítica

Recursos afectados:

- Cisco Jabber para Windows, versiones:
  - 12.1 y anteriores;
  - 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 12.9 y anteriores.

Descripción:

Cisco ha publicado 5 vulnerabilidades, 1 de severidad crítica, 1 alta y 3 medias, que podrían permitir a un atacante ejecutar programas arbitrarios con privilegios elevados, acceder a información sensible, interceptar el tráfico de red protegido o provocar una condición de denegación de servicio (DoS).

Solución:

Actualizar las versiones afectadas a las siguientes versiones corregidas:

- Cisco Jabber para Windows:
  - anteriores a 12.1: actualizar a una versión corregida;
  - 12.1: actualizar a 12.1.5;
  - 12.5: actualizar a 12.5.4;
  - 12.6: actualizar a 12.6.5;
  - 12.7: actualizar a 12.7.4;
  - 12.8: actualizar a 12.8.5;
  - 12.9: actualizar a 12.9.5.
- Cisco Jabber para MacOS:
  - 12.7 y anteriores: actualizar a una versión corregida;
  - 12.8: actualizar a 12.8.7;
  - 12.9: actualizar a 12.9.6.

- Cisco Jabber para Android e iOS, versiones 12.9 y anteriores: actualizar a una versión corregida.

Detalle:

- Una vulnerabilidad en Cisco Jabber para Windows podría permitir a un atacante, remoto y autenticado, ejecutar código arbitrario en un sistema mediante el envío de mensajes XMPP especialmente diseñados. Se ha asignado el identificador CVE-2021-1411 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2021-1417, CVE-2021-1418, CVE-2021-1469 y CVE-2021-1471.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

---

Múltiples vulnerabilidades en OpenSSL

Fecha de publicación: 26/03/2021

Importancia: Alta

Recursos afectados:

- OpenSSL 1.1.1h y versiones posteriores están afectadas por la vulnerabilidad CVE-2021-3450;
- todas las versiones de OpenSSL 1.1.1 están afectadas por la vulnerabilidad CVE-2021-3449.

NOTA: las versiones 1.0.2 y 1.1.0 ya no reciben soporte ni actualizaciones, por lo que los usuarios deben actualizar a la versión 1.1.1.

Descripción:

Investigadores, de Akamai y Nokia, reportaron a OpenSSL 2 vulnerabilidades, ambas con severidad alta, de tipo denegación de servicio (DoS) y validación inadecuada del certificado de la Autoridad de Certificación (CA).

Solución:

Actualizar OpenSSL a la versión 1.1.1k.

Detalle:

- Esta vulnerabilidad podría permitir eludir por completo la verificación de un certificado, al no comprobar correctamente la validez de los certificados. Solo afecta si se ha activado el flag *X509_V_FLAG_X509_STRICT* (no está activo por defecto). Se ha asignado el identificador CVE-2021-3450 para esta vulnerabilidad.
- Un servidor TLS de OpenSSL podría fallar si se le envía un mensaje de renegociación *ClientHello* de un cliente, lo que generaría una condición de DoS. Un servidor sólo es vulnerable si tiene TLSv1.2 y la renegociación activada (configuración por defecto). Los clientes TLS de OpenSSL no se ven afectados por este problema. Se ha asignado el identificador CVE-2021-3449 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, SSL/TLS, Vulnerabilidad

---

Vulnerabilidad 0day en productos de Apple

Fecha de publicación: 29/03/2021

Importancia: Crítica

Recursos afectados:

- iOS, versiones anteriores a 12.5.2 y 14.4.2;
- iPadOS, versiones anteriores a 14.4.2;
- watchOS, versiones anteriores a 7.3.3.

Descripción:

Clement Lecigne y Billy Leonard, investigadores de Google Threat Analysis Group, han informado a Apple de una vulnerabilidad 0day, que podría permitir a un atacante realizar un XSS.

Solución:

Actualizar a las versiones referenciadas, siguiendo los pasos indicados en la web oficial del fabricante y que están disponibles para los siguientes productos:

- iOS 14.4.2 y iPadOS 14.4.2:
  - iPhone 6s y posteriores,
  - iPad Pro (todos los modelos),
  - iPad Air 2 y posteriores,
  - iPad 5ª generación y posteriores,
  - iPad mini 4 y posteriores,
  - iPod touch (7ª generación).
- iOS 12.5.2:
  - iPhone 5s,
  - iPhone 6,
  - iPhone 6 Plus,

    - iPad Air,
    - iPad mini 2,
    - iPad mini 3,
    - iPod touch (6ª generación).
- watchOS 7.3.3: Apple Watch Series 3 y posteriores.

Detalle:

El procesamiento en WebKit de contenido web potencialmente peligroso podría permitir un XSS (*Cross Site Scripting*) universal. Este problema se ha solucionado con una mejor gestión del ciclo de vida de los objetos. Apple ha informado de que esta vulnerabilidad puede haber sido explotada activamente. Se ha asignado el identificador CVE-2021-1879 para esta vulnerabilidad.

Etiquetas: 0day, Actualización, Apple, Vulnerabilidad

Múltiples vulnerabilidades en Orion Platform de SolarWinds

Fecha de publicación: 29/03/2021

Importancia: Crítica

Recursos afectados:

Orion Platform, versiones anteriores a la 2020.2.5.

Descripción:

ZDI Trend Micro y los investigadores Jhon Jaro y Harrison Neal han reportado a SolarWinds una vulnerabilidad de severidad crítica, dos vulnerabilidades de severidad alta y otra de severidad media, que podrían permitir a un atacante la ejecución remota de código, realizar ataques mediante XSS almacenado, *tabnabbing* inverso o redireccionamiento abierto.

Solución:

Actualizar Orion Platform a la versión 2020.2.5.

Detalle:

- Un atacante remoto autenticado podría ejecutar código a través de acciones para la comprobación de alertas.
- Un atacante remoto, con conocimiento de las credenciales de una cuenta local sin privilegios en un servidor Orion, podría ejecutar código con privilegios de administrador.
- Un atacante con cuenta de administrador de Orion podría explotar una vulnerabilidad XSS almacenada presente en la pestaña de añadir personalización en la página de personalización. Se ha asignado el identificador CVE-2020-35856 para esta vulnerabilidad de severidad alta.
- Un atacante con cuenta de administrador de Orion podría explotar una vulnerabilidad de *tabnabbing* inverso y redireccionamiento abierto en la página de opciones de personalización. Se ha asignado el identificador CVE-2021-3109 para esta vulnerabilidad de severidad media.

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

---

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 31/03/2021

Importancia: Crítica

Recursos afectados:

- vRealize Operations Manager, versiones:
    - 8.3.0;
    - 8.2.0;
    - 8.1.1, 8.1.0;
    - 8.0.1, 8.0.0;
    - 7.5.0.
- VMware Cloud Foundation (vROps), versiones:
    - 4.x;
    - 3.x.
- vRealize Suite Lifecycle Manager (vROps), versiones 8.x.

Descripción:

Egor Dimitrenko, investigador de Positive Technologies, ha reportado 2 vulnerabilidades críticas a VMware, de tipos SSRF (*Server Side Request Forgery*) y escritura arbitraria de archivos.

Solución:

Aplicar los siguientes parches, en función de la versión de producto afectada:

- vRealize Operations Manager:
    - 8.3.0: KB83210;

    - 8.2.0: KB83095;
    - 8.1.1, 8.1.0: KB83094;
    - 8.0.1, 8.0.0: KB83093;
    - 7.5.0: KB82367.
- VMware Cloud Foundation (vROps):
    - 4.x: KB83260;
    - 3.x: KB83260.
- vRealize Suite Lifecycle Manager (vROps), versiones 8.x: KB83260.

Detalle:

- Un atacante, con acceso a la red, a la API de vRealize Operations Manager, podría realizar un ataque SSRF (*Server Side Request Forgery*) para robar credenciales administrativas. Se ha asignado el identificador CVE-2021-21975 para esta vulnerabilidad.
- Un atacante autenticado, con acceso a la red, a la API de vRealize Operations Manager, podría escribir archivos en ubicaciones arbitrarias en el sistema operativo subyacente *photon*. Se ha asignado el identificador CVE-2021-21983 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad