Boletín de agosto de 2020

Avisos Técnicos

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Vulnerabilidad de inyección de comandos en NETGEAR R8300

Fecha de publicación: 03/08/2020

Importancia: Crítica

Recursos afectados:

Router NETGEAR R8300, versiones de *firmware* anteriores a 1.0.2.134.

Descripción:

Un investigador independiente ha reportado a NETGEAR una vulnerabilidad, de severidad crítica, de tipo inyección de comandos, que afecta al router NETGEAR R8300.

Solución:

Descargar la útltima versión disponible de *firmware* del producto afectado.

Detalle:

NETGEAR ha solucionado una vulnerabilidad de seguridad, reportada al fabricante a través del programa SSD Secure Disclosure, de tipo inyección de comandos previa a la autenticación en su modelo de router R8300.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Actualización de seguridad de SAP de agosto de 2020

Fecha de publicación: 12/08/2020

Importancia: Crítica

Recursos afectados:

- SAP NetWeaver AS JAVA (LM Configuration Wizard), versiones 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver (Knowledge Management), versiones 7.30, 7.31, 7.40 y 7.50;
- SAP Business Objects Business Intelligence Platform, versiones 4.2 y 4.3;
- SAP Banking Services (Generic Market Data), versiones 400, 450 y 500;
- SAP NetWeaver (ABAP Server) y ABAP Platform, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 753 y 755;
- SAP NetWeaver AS JAVA (ENGINEAPI), versiones 7.10 y 7.10;
- SAP NetWeaver AS JAVA (WSRM), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver AS JAVA (SERVERCORE), versiones 7.10, 7.10 y 7.11;
- SAP NetWeaver AS JAVA (J2EE-FRMW), versiones J2EE-FRMW 7.10 y 7.11;
- SAP NetWeaver (Knowledge Management), versiones 7.30, 7.31, 7.40 y 7.50;
- SAP Adaptive Server Enterprise, versión 16.0;
- SAP Commerce, versiones 6.7, 1808, 1811, 1905 y 2005;
- SAP Data Intelligence, versión 3;
- SAPUI5 (UISAPUI5_JAVA), versión 7.50;
- SAPUI5 (SAP_UI), versiones 750, 751, 752, 753, 754 y 755;
- SAPUI5 (UI_700), versión 200;
- SAP ERP (HCM Travel Management), versiones 600, 602, 603, 604, 605, 606, 607 y 608;
- SAP Business Objects Business Intelligence Platform (Central Management Console), versiones 4.2 y 4.3;
- SAP S/4 HANA (Fiori UI for General Ledger Accounting), versiones 103 y 104;
- SAP NetWeaver (ABAP Server) y ABAP Platform, versiones 740, 750, 751, 752, 753, 754 y 755;
- SAP NetWeaver (ABAP Server) y ABAP Platform, versiones 702, 730, 731, 740 y 750.

Descripción:

SAP ha publicado varias actualizaciones de seguridad de diferentes productos en su comunicado mensual.

Solución:

Visitar el portal de soporte de SAP e instalar las actualizaciones o los parches necesarios, según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 15 notas de seguridad y 1 actualización, siendo 2 de ellas de severidad crítica, 6 altas y 8 medias.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 1 vulnerabilidad de inyección de código,
- 5 vulnerabilidades de *Cross-Site Scripting*,
- 4 vulnerabilidades de divulgación de información,
- 3 vulnerabilidades de falta de comprobación de autorización,
- 4 vulnerabilidades de falta de comprobación de autenticación,
- 1 vulnerabilidad de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- La falta de comprobación de autenticación en SAP NetWeaver AS JAVA (LM Configuration Wizard) podría permitir a un atacante, sin autenticación previa, ejecutar tareas de configuración para realizar acciones críticas contra el sistema SAP Java, incluyendo la capacidad de crear un usuario administrativo, y por lo tanto comprometiendo la confidencialidad, integridad y disponibilidad del sistema. Se ha asignado el identificador CVE-2020-6287 para esta vulnerabilidad.

- Una vulnerabilidad de tipo Cross-Site Scripting (XSS) que afecta a SAP Knowledge Management, un componente de SAP NetWeaver, específicamente de SAP Enterprise Portal, y que puede suponer un compromiso total de la confidencialidad, integridad y disponibilidad del sistema. Se ha asignado el identificador CVE-2020-6284 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-6294, CVE-2020-6298, CVE-2020-6296, CVE-2020-6309, CVE-2020-6293, CVE-2020-6295, CVE-2020-6297, CVE-2020-6301, CVE-2020-6300, CVE-2020-6273, CVE-2020-6299 y CVE-2020-6310.

Etiquetas: Actualización, SAP, Vulnerabilidad

Boletín de seguridad de Microsoft de agosto de 2020

Fecha de publicación: 12/08/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Scripting Engine
- SQL Server
- Microsoft JET Database Engine
- .NET Framework
- ASP.NET Core
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Microsoft Dynamics

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de agosto, consta de 124 vulnerabilidades, 14 clasificadas como críticas y 103 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de Microsoft se informa de los distintos métodos para llevar a cabo dichas actualizaciones.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- escalada de privilegios,
- denegación de servicio,
- ejecución remota de código,
- divulgación de información,
- suplantación de identidad (spoofing).

IMPORTANTE: Microsoft ha informado de que dos vulnerabilidades estarían siendo explotadas por acatantes de manera activa, en concreto una vulnerabilidad de ejecución remota de código que afecta a Internet Explorer 11, a la que se ha asignado el identificador CVE-2020-1380, la otra vulnerabilidad se refiere a una suplantación de identidad que afecta a varios productos de Windows y a la que se ha asignado el identificador CVE-2020-1464.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en Intel Server Boards, Server Systems y Compute Modules

Fecha de publicación: 12/08/2020

Importancia: Crítica

Recursos afectados:

- Intel Server System R1000WT, R2000WT, R1000SP, LSVRP, LR1304SP, R1000WF y R2000WF,
- Intel Server Boards S2600WT, S2600CW, S2600KP, S2600TP, S1200SP, S2600WF, S2600ST y S2600BP,
- Intel Compute Module HNS2600KP, HNS2600TP y HNS2600BP.

Descripción:

Intel ha informado de múltiples vulnerabilidades en sistemas Intel Server System, Server Boards y Compute Module que podrían permitir a un atacante realizar una escalada de privilegios o una denegación de servicio.

Solución:

Intel ha publicado una nueva versión de firmware para los productos afectados. Puede consultar la lista detallada en su página web.

Detalle:

Se han encontrado un total de 22 vulnerabilidades siendo 1 de ellas de importancia crítica y 10 de importancia alta.

La vulnerabilidad más crítica se refiere a un fallo en los sistema de autenticación en algunas placas Intel Server Boards, Server Systems y Compute Modules anteriores a la versión 1.59, la cual puede permitir a un atacante no autenticado llevar a cabo una escalada de privilegios a través de un acceso adyacente. Se ha reservado el identificador CVE-2020-8708 para esta vulnerabilidad.

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en Citrix Endpoint Management (CEM)

Fecha de publicación: 13/08/2020

Importancia: Crítica

Recursos afectados:

- XenMobile Server 10.12, versiones anteriores a RP3,
- XenMobile Server 10.11, versiones anteriores a RP6,
- XenMobile Server 10.10, versiones anteriores a RP6
- XenMobile Server 10.9, versiones anteriores a RP5.

Descripción:

Investigadores de Positive Technologies, Tradecraft y Detectify ha reportado varias vulnerabilidades críticas que afectan a Citrix Endpoint Management (CEM), también conocido como XenMobile. Estas vulnerabilidades podrían permitir a un atacante no autenticado obtener privilegios administrativos en el dispositivo.

Solución:

Citrix ha publicado parches para las siguientes versiones:

- XenMobile Server 10.12 RP3,
- XenMobile Server 10.11 RP6,
- XenMobile Server 10.10 RP6,
- XenMobile Server 10.9 RP5.

Detalle:

Citrix no ha compartido detalles técnicos sobre las vulnerabilidades encontradas, pero desde Positive Technologies se ha informado de que al menos una de las vulnerabilidades consistiría en un salto de ruta o Path Traversal, y que permitiría a un atacante leer archivos

arbitrarios fuera del directorio raíz del servidor web, incluidos archivos de configuración y claves de cifrado para datos confidenciales. Se ha reservado el identificador CVE-2020-8209 para esta vulnerabilidad calificada como crítica.

Otros identificadores reservados para estas vulnerabilidades son: CVE-2020-8208, también calificado como crítico y CVE-2020-8210, CVE-2020-8211 y CVE-2020-8212, con criticidades medias o bajas.

Etiquetas: Actualización, Comunicaciones, Virtualización, Vulnerabilidad

---

Múltiples vulnerabilidades en Apache Struts 2

Fecha de publicación: 17/08/2020

Importancia: Alta

Recursos afectados:

Apache Struts 2, versiones desde 2.0.0 hasta 2.5.20.

Descripción:

Matthias Kaiser, de Apple Information Security, y Takeshi Terada, de Mitsui Bussan Secure Directions Inc., han reportado 2 vulnerabilidades, de severidad alta y media, de tipo ejecución remota de código y denegación de servicio, respectivamente.

Solución:

Apache Struts 2 a la versión 2.5.22.

Detalle:

- Los *frameworks* de Apache Struts, cuando se fuerza la comprobación, realizan una doble evaluación de los valores de los atributos asignados a ciertos atributos de etiquetas, como por ejemplo *id*, por lo que sería posible pasar un valor que se evaluará nuevamente cuando se muestren los atributos de una etiqueta. Este problema solo aplica cuando se fuerza la evaluación OGNL dentro de un atributo de etiqueta de Struts, cuando la expresión para evaluar hace referencia a una entrada sin validar y sin procesar que un atacante podría modificar directamente, creando la solicitud correspondiente y generando una posible situación de ejecución remota de código (RCE). Se ha reservado el código CVE-2019-0230 para esta vulnerabilidad.

Para la otra vulnerabilidad se ha reservado el identificador CVE-2019-0233.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades afectan al core de Jenkins

Fecha de publicación: 18/08/2020

Importancia: Crítica

Recursos afectados:

- Jenkins hasta versión 2.251 inclusive;
- Jenkins LTS hasta versión 2.235.4 inclusive.

Descripción:

Diversos investigadores han informado de múltiples vulnerabilidades que afectan al *core* de Jenkins, concretamente 1 es de severidad crítica y 3 altas, de tipo corrupción en el buffer y *Cross-Site Scripting* (XSS) almacenado, respectivamente.

Solución:

Se recomienda instalar las siguientes versiones para solucionar estas vulnerabilidades:

- Jenkins versión 2.252;
- Jenkins LTS versión 2.235.5.

Detalle:

- Jenkins incluye Winstone-Jetty, un *wrapper* de Jetty, para que actúe como HTTP y *servlet*, que contiene una vulnerabilidad que podría permitir que atacantes no autenticados obtengan encabezados de respuesta HTTP con datos confidenciales destinados a otro usuario. Se ha asignado el identificador CVE-2019-17638 para esta vulnerabilidad.
- Jenkins no sanitiza correctamente el contenido de información sobre herramientas de los iconos de ayuda, la descripción de la estrategia de nomenclatura del proyecto que se muestra en la creación del artículo, ni la dirección remota del *host* que inicia una compilación a través de *Trigger builds remotely*, lo que podría conducir a vulnerabilidades de XSS. Se han asignado los identificadores CVE-2020-2229, CVE-2020-2230 y CVE-2020-2231 para estas vulnerabilidades.

Además, Jenkins ha informado de otras vulnerabilidades en diferentes complementos.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en HP-UX CIFS de HPE

Fecha de publicación: 19/08/2020

Importancia: Crítica

Recursos afectados:

HP-UX Common Internet File System (CIFS) Client/Server Software, versión B.04.09.00.00 y anteriores.

Descripción:

El equipo de respuesta de seguridad de productos HPE ha reportado 4 vulnerabilidades, 1 de severidad crítica y el resto medias, de tipo limitación incorrecta del nombre de ruta a un directorio restringido (*path traversal*) y lectura fuera de límites.

Solución:

Actualizar HP-UX CIFS Client/Server Software a la versión B.04.12.03.00.

Detalle:

- Un atacante, tanto local como remoto, podría aprovechar la vulnerabilidad crítica para escapar del directorio compartido y acceder a información no autorizada. Se ha asignado el identificador CVE-2019-10197 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores CVE-2019-10218, CVE-2019-14907 y CVE-2019-3880.

Etiquetas: Actualización, HP, Vulnerabilidad

Uso de credenciales por defecto en varios productos de Cisco

Fecha de publicación: 20/08/2020

Importancia: Crítica

Recursos afectados:

Esta vulnerabilidad afecta a los dispositivos de las series Cisco ENCS 5400-W y CSP 5000-W si ejecutan Cisco vWAAS con versiones 6.4.5 o 6.4.3d y anteriores de imágenes empaquetadas de NFVIS.

Descripción:

Esta vulnerabilidad, que se encontró durante las pruebas de seguridad internas, posee una severidad crítica y es de tipo uso de credenciales por defecto y estáticas.

Solución:

Cisco solucionó esta vulnerabilidad en Cisco vWAAS con la publicación de las versiones 6.4.3e, 6.4.5a y versiones posteriores de la imagen empaquetada NFVIS, disponibles en el centro de descargas de Cisco.

NOTA: los dispositivos de la serie ENCS 5400-W y CSP 5000-W no admiten una actualización directa a las versiones vWAAS 6.4.3e y 6.4.5a de versiones anteriores. Para ejecutar una versión ya corregida, los clientes deben realizar una instalación nueva con la versión requerida del paquete unificado de Cisco WAAS para dispositivos ENCS 5400-W y CSP 5000-W.

Detalle:

Un atacante remoto, no autenticado, podría acceder al CLI (*Command Line Interface*) del NFVIS (*NFV Infrastructure Software*) de un producto afectado utilizando cuentas con credenciales por defecto, pudiendo obtener de esta manera privilegios de administrador. Se ha reservado el identificador CVE-2020-3446 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Xen, Citrix Hypervisor y XenServer

Fecha de publicación: 25/08/2020

Importancia: Alta

Recursos afectados:

- Todas las versiones de Xen;
- Citrix Hypervisor 8.2 LTSR;
- Citrix Hypervisor 8.1;
- Citrix Hypervisor 8.0;
- Citrix XenServer 7.1 LTSR CU2;
- Citrix XenServer 7.0.

Descripción:

Se ha informado de varias vulnerabilidades que afectan a QEMU y que podrían permitir a un atacante la ejecución de código en una VM invitada con los privilegios del Proceso QEMU en el *host* o en una denegación de servicio (DoS) en el servicio.

Solución:

Se recomienda instalar las siguientes versiones:

- Parche disponible para Xen;
- Citrix Hypervisor 8.2 LTSR: CTX280214;
- Citrix Hypervisor 8.1: CTX280213;

- Citrix Hypervisor 8.0: CTX280212;
- Citrix XenServer 7.1 LTSR CU2: CTX280211;
- Citrix XenServer 7.0: CTX280210.

Detalle:

Se han identificado vulnerabilidades en QEMU que afectan a Citrix Hypervisor y a Xen, permitiendo el acceso de lectura/escritura fuera de los límites en el emulador USB de la QEMU y provocando en ciertas configuraciones la ejecución de código privilegiado en una VM invitada, comprometiendo potencialmente el *host*.

Las vulnerabilidades publicadas tienen asignados los siguientes identificadores: CVE-2018-17958 y CVE-2020-14364.

Etiquetas: Actualización, Virtualización, Vulnerabilidad