Boletín de noviembre de 2020

Avisos Técnicos

Vulnerabilidad de ejecución remota de código en Oracle WebLogic Server

Fecha de publicación: 03/11/2020

Importancia: Crítica

Recursos afectados:

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.

Descripción:

Diversos investigadores y equipos de seguridad han reportado esta vulnerabilidad, de severidad crítica, de tipo ejecución remota de código que afecta a Oracle WebLogic Server.

Solución:

Seguir las instrucciones descritas en el documento de disponibilidad de parches *Fusion Middleware* (requiere *login*).

Detalle:

Esta vulnerabilidad, que está relacionada con CVE-2020-14882, que ya se abordó en las actualizaciones críticas en Oracle (octubre 2020), es fácilmente explotable y podría permitir que un atacante no autenticado, con acceso a la red a través de HTTP, comprometa Oracle WebLogic Server. Se ha asignado el identificador CVE-2020-14750 para esta vulnerabilidad.

Etiquetas: Actualización, Java, Oracle, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en el kernel de Windows

Fecha de publicación: 03/11/2020

Importancia: Crítica

Recursos afectados:

Todas las versiones de Windows, desde Windows 7, hasta la versión más reciente de Windows 10.

Descripción:

Mateusz Jurczyk y Sergei Glazunovl, del equipo de Google Project Zero, han descubierto una vulnerabilidad de 0-day en el sistema operativo Windows que actualmente podría estar siendo explotada de forma activa, permitiendo la escalada de privilegios.

Solución:

- La actualización que corrige esta vulnerabilidad de 0-day de Windows se publicará el dia 10 de noviembre.
- La vulnerabilidad de Google Chrome fue parcheada en la versión 86.0.4240.111.

Detalle:

El controlador de criptografía del *kernel* de Windows, Windows Kernel Cryptography Driver (*cng.sys*), expone un dispositivo *DeviceCNG* a programas en modo usuario y admite una variedad de IOCTL con estructuras de entrada no triviales, lo que podría permitir a un atacante, local, escalar privilegios y salir de la *sandbox*. Se ha asignado el identificador CVE-2020-17087 para esta vulnerabilidad.

Para poder llevar a cabo la explotación de esta vulnerabilidad, los atacantes están utilizando previamente la vulnerabilidad de 0-day en Google Chrome, cuyo identificador asignado es CVE-2020-15999, que les permite ejecutar código malicioso dentro de Chrome.

Etiquetas: 0day, Vulnerabilidad, Windows

Múltiples vulnerabilidades en Salt de SaltStack

Fecha de publicación: 05/11/2020

Importancia: Crítica

Recursos afectados:

Salt, versión 3002 y anteriores.

Descripción:

KPC, de Trend Micro Zero Day Initiative, ha reportado 2 de las 3 vulnerabilidades detectadas. 2 de estas vulnerabilidades tienen severidad alta/crítica y 1 baja, y son de tipo inyección de comandos, omisión de autenticación y problema de permisos.

Solución:

Las siguientes versiones tendrán un paquete disponible para descargar desde el repositorio:

- 3002.x;
- 3001.x;
- 3000.x;
- 2019.x.

Las siguientes versiones tendrán un parche disponible para descargar:

- 3002;
- 3001.1 y 3001.2;
- 3000.3 y 3000.4;
- 2019.2.5 y 2019.2.6;
- 2018.3.5;
- 2017.7.4 y 2017.7.8;
- 2016.11.3, 2016.11.6 y 2016.11.10;
- 2016.3.4, 2016.3.6 y 2016.3.8;
- 2015.8.10 y 2015.8.13.

Detalle:

- Un usuario, no autenticado, con acceso de red a la API de Salt, podría realizar inyecciones de comandos (*shell injections*) para ejecutar código en la API de Salt mediante el cliente SSH. Se ha asignado el identificador CVE-2020-16846 para esta vulnerabilidad.
- Cuando se usa el cliente SSH, un usuario no autenticado podría obtener acceso para ejecutar comandos contra objetivos establecidos en una lista Salt-SSH, debido a que *eauth* no se valida correctamente al llamar al cliente SSH a través de la API, por lo que cualquier valor para *eauth* o *token* permitiría al usuario omitir la autenticación. Se ha asignado el identificador CVE-2020-25592 para esta vulnerabilidad.

Para la vulnerabilidad de severidad baja, se ha asignado el identificador CVE-2020-17490.

Etiquetas: Actualización, Vulnerabilidad

Escalada de privilegios en HPE OneView y Synergy Composer

Fecha de publicación: 05/11/2020

Importancia: Crítica

Recursos afectados:

- HPE Synergy Composer, versiones 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4 y anteriores;
- HPE Synergy Composer2, versiones 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4;
- HP OneView, versiones 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4 y anteriores.

Descripción:

Hewlett Packard Enterprise ha publicado una vulnerabilidad que podría permitir a un atacante la escalada remota de privilegios.

Solución:

Actualizar a la versión 5.5 de OneView, Composer y Composer2.

Detalle:

La vulnerabilidad podría permitir a un atacante, siendo usuario de una cuenta OneView en OneView y Synergy Composer, realizar una escalada de privilegios de forma remota. Se ha asignado el identificador CVE-2020-7198 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Validación de entrada incorrecta en Cisco AnyConnect Secure Mobility Client

Fecha de publicación: 05/11/2020

Importancia: Alta

Recursos afectados:

Esta vulnerabilidad afecta a todas las versiones del *software* Cisco AnyConnect Secure Mobility Client con una configuración vulnerable para las siguientes plataformas:

- AnyConnect Secure Mobility Client para Linux,
- AnyConnect Secure Mobility Client para MacOS,
- AnyConnect Secure Mobility Client para Windows.

Una configuración vulnerable requiere que se habiliten, tanto la configuración *Auto Update* (habilitada predeterminadamente), como *Enable Scripting* (deshabilitada de manera predeterminada).

Descripción:

Gerbert Roitburd, investigador de Secure Mobile Networking Lab (TU Darmstadt), ha notificado una vulnerabilidad, con severidad alta, de tipo validación de entrada incorrecta.

Solución:

Cisco no ha publicado actualizaciones de *software* que aborden esta vulnerabilidad. El PSIRT (*Product Security Incident Response Team*) del fabricante es consciente de que el código de explotación de PoC está disponible para la vulnerabilidad descrita en este aviso, aunque no tiene conocimiento de ningún uso malintencionado de la vulnerabilidad descrita.

Una mitigación para esta vulnerabilidad es deshabilitar la funcionalidad *Auto Update*.

Detalle:

Una vulnerabilidad en IPC (*Interprocess Communication Channel*) del *software* Cisco AnyConnect Secure Mobility Client podría permitir que un atacante local, autenticado, haga que un usuario de AnyConnect ejecute un *script* malicioso, enviando mensajes IPC, especialmente diseñados, al oyente IPC del cliente AnyConnect. Se ha asignado el identificador CVE-2020-3556 para esta vulnerabilidad.

Etiquetas: Cisco, Comunicaciones, Vulnerabilidad

Actualizaciones de seguridad de Microsoft de noviembre de 2020

Fecha de publicación: 11/11/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Internet Explorer;

- Microsoft Edge (basado en EdgeHTML),
- Microsoft Edge (basado en Chromium);
- ChakraCore;
- Microsoft Exchange Server;
- Microsoft Dynamics;
- Microsoft Windows Codecs Library;
- Azure Sphere;
- Windows Defender;
- Microsoft Teams;
- Azure SDK;
- Azure DevOps;
- Visual Studio.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de noviembre, consta de 104 vulnerabilidades, 16 clasificadas como críticas, 86 como importantes y 2 bajas.

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*).
- manipulación (*tampering*).

Etiquetas: Actualización, Comunicaciones, Microsoft, Navegador, Vulnerabilidad

---

Vulnerabilidad de escalada de privilegios en la instalación de LogicalDoc

Fecha de publicación: 11/11/2020

Importancia: Crítica

Recursos afectados:

LogicalDoc 8.5.1

Descripción:

El investigador, Yuri Kramarz, de Cisco Talos ha descubierto una vulnerabilidad de escalada de privilegios en la instalación del sistema de gestión de documentos, LogicalDoc. Un atacante podría reemplazar cualquiera de los archivos DLL de la carpeta de instalación cargados por la aplicación y obtener privilegios de SYSTEM.

Solución:

Se recomienda actualizar a la versión 8.5.2.

Detalle:

La vulnerabilidad encontrada permite una escalada de privilegios debido a que la carpeta de instalación por defecto es 'C:LogicalDOC' y permite a usuarios autenticados en el sistema modificar ficheros que luego son ejecutados con privilegios de SYSTEM authority, produciéndose así la escalada de privilegios en el sistema. Se ha asignado el identificador CVE-2020-13542 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Escalada de privilegios en productos Intel

Fecha de publicación: 11/11/2020

Importancia: Crítica

Recursos afectados:

- Intel® CSME e Intel® AMT, versiones anteriores a las 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 y 14.5.25;
- Intel® TXE, versiones anteriores a la 3.1.80 y la 4.0.30;
- Intel® Server Platform Services, versiones de *firmware* anteriores a SPS_E5_04.01.04.400, SPS_E3_05.01.04.200, SPS_E3_04.01.04.200, SPS_SoC-X_04.00.04.200 y SPS_SoC-A_04.00.04.300.

- Las versiones de firmware de Intel® ME 3.x a 10.x, Intel® TXE 1.x a 2.x e Intel® Server Platform Services 1.x a 2.X ya no son versiones compatibles. No hay nuevos lanzamientos planeados para estas versiones.
- Intel® Wireless Bluetooth®:
  - Intel® Wi-Fi 6 AX201,
  - Intel® Wi-Fi 6 AX200,
  - Intel® Wireless-AC 9560,
  - Intel® Wireless-AC 9462,
  - Intel® Wireless-AC 9461,
  - Intel® Wireless-AC 9260,
  - Intel® Dual Band Wireless-AC 8265,
  - Intel® Dual Band Wireless-AC 8260,
  - Intel® Dual Band Wireless-AC 3168,
  - Intel® Wireless 7265 (Rev D) Family,
  - Intel® Dual Band Wireless-AC 3165.

Descripción:

Intel ha publicado 2 vulnerabilidades, de severidad crítica, del tipo lectura fuera de límites y restricción incorrecta del búfer.

Solución:

- Para usuarios de Intel® CSME, Intel® TXE, Intel® AMT e Intel® SPS, se recomienda actualizar a la última versión.
- Intel® AMT SDK, está disponible para su descarga.
- Intel® DAL SDK, se encuentra sin soporte, se recomienda dejar de utilizarlo y desinstalarlo.
- Actualizar los productos Intel® Wireless Bluetooth® a la versión 21.110 o posterior.

Detalle:

- La escritura fuera de los límites, en el subsistema IPv6, podría permitir a un atacante no autenticado la escalada de privilegios a través del acceso a la red. Se ha asignado el identificador CVE-2020-8752 para esta vulnerabilidad.
- La restricción incorrecta del búfer podría permitir a un atacante no autenticado, la escalada de privilegios a través de un acceso adyacente. Se ha asignado el identificador CVE-2020-12321 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de noviembre de 2020

Fecha de publicación: 11/11/2020

Importancia: Crítica

Recursos afectados:

- SAP Solution Manager (JAVA stack y User Experience Monitoring), versión 7.2;
- SAP Data Services, versión 4.2;
- SAP AS ABAP(DMIS), versiones 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752 y 2020;
- SAP S4 HANA, versiones 100, 101, 102, 103, 104 y 105;
- SAP NetWeaver, versiones 7.20, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55 y 7.82;
- SAP Fiori Launchpad (News Tile Application), versiones 750, 751, 752, 753, 754 y 755;
- SAP Commerce Cloud, versiones 1808, 1811, 1905 y 2005;
- BANKING SERVICES FROM SAP 9.0 (Bank Analyzer), versión 500;
- S/4HANA FIN PROD SUBLDGR, versión 100;
- SAP Process Integration (PGP Module ? Business-to-Business Add On), versión 1.0;
- SAP ERP Client para E-Bilanz 1.0, versión 1.0;
- SAP ERP, versiones 600, 602, 603, 604, 605, 606, 616, 617 y 618;
- SAP 3D Visual Enterprise Viewer, versión 9.

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 12 notas de seguridad y 3 actualizaciones de notas anteriores, siendo 6 de las nuevas notas de severidad crítica, 3 altas y 6 medias.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 5 vulnerabilidades de falta de comprobación de autenticación,
- 4 vulnerabilidades de divulgación de información,
- 3 vulnerabilidades de falta de comprobación de autorización,
- 2 vulnerabilidades de denegación de servicio (DoS),
- 1 vulnerabilidad de inyección de código,
- 1 vulnerabilidad de inyección de comandos en el SSOO,
- 1 vulnerabilidad de ejecución remota de código (RCE),
- 4 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Estas vulnerabilidades críticas, de falta de autenticación, tienen un impacto negativo en la integridad y disponibilidad del servicio LM-Service, así como de cuatro servicios dependientes. Se han asignado los identificadores CVE-2020-26821, CVE-2020-26822, CVE-2020-26823 y CVE-2020-26824 para estas vulnerabilidades.
- SAP Solution Manager, debido a la falta de verificación de autenticación, no realiza ninguna autenticación para un servicio, lo que podría resultar en un compromiso completo de todos los agentes SMDA conectados al Solution Manager. Se ha asignado el identificador CVE-2020-6207 para esta vulnerabilidad.
- Una validación de entrada insuficiente podría permitir que un atacante, no autenticado, enviase solicitudes maliciosas que podrían resultar en la ejecución remota de código y, por lo tanto, en un compromiso total de la confidencialidad, integridad y disponibilidad del sistema. Se han asignado los identificadore CVE-2019-0230 y CVE-2019-0233 para estas vulnerabilidades.
- SAP AS ABAP (DMIS) podría permitir a un atacante autenticado inyectar código arbitrario en el módulo de función, lo que resultaría en una inyección de código que se podría ejecutar en la aplicación, afectando a la confidencialidad, disponibilidad e integridad de la aplicación. Se ha asignado el identificador CVE-2020-26808 para esta vulnerabilidad.
- El parche corrige un error en SAP NetWeaver Application Server Java que podría permitir que los usuarios autenticados en SAP escalasen a los comandos del sistema operativo en el vulnerable y, por lo tanto, lograsen comprometer totalmente cada servicio y pieza de información en ejecución. Se ha asignado el identificador CVE-2020-26820 para esta vulnerabilidad.
- SAP NetWeaver (Knowledge Management) podría permitir la ejecución automática del contenido del *script* en un archivo almacenado debido a un filtrado inadecuado con los privilegios del usuario que accede. Si dicho usuario tiene privilegios administrativos, entonces la ejecución del contenido del *script* podría resultar en un compromiso total de la confidencialidad, integridad y disponibilidad del sistema, lo que conduciría a un XSS almacenado. Se ha asignado el identificador CVE-2020-6284 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-26825, CVE-2020-26809, CVE-2020-26811, CVE-2020-26819, CVE-2020-6311, CVE-2020-26814, CVE-2020-26807, CVE-2020-6316 y CVE-2020-26817.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en Citrix SD-WAN Center

Fecha de publicación: 12/11/2020

Importancia: Crítica

Recursos afectados:

- Citrix SD-WAN 11.2, versiones anteriores a 11.2.2;
- Citrix SD-WAN 11.1, versiones anteriores a 11.1.2b;
- Citrix SD-WAN 10.2, versiones anteriores a 10.2.8.

Descripción:

Ariel Tempelhof, investigador de Realmode Labs, ha notificado 3 vulnerabilidades, de severidad crítica, de tipo limitación inadecuada de una ruta de acceso a un directorio restringido (*path transversal*), autenticación inadecuada e inyección de comandos del sistema operativo.

Solución:

Las vulnerabilidades se han solucionado en las siguientes versiones de Citrix SD-WAN Center:

- Citrix SD-WAN 11.2.2 y versiones posteriores de Citrix SD-WAN 11.2;
- Citrix SD-WAN 11.1.2b y versiones posteriores de Citrix SD-WAN 11.1;
- Citrix SD-WAN 10.2.8 y versiones posteriores de Citrix SD-WAN 10.2.

Detalle:

- Un atacante, que pueda comunicarse con la dirección IP / FQDN de SD-WAN Center, podría realizar una ejecución de código remoto, no autenticado, con privilegios de *root*. Se ha asignado el identificador CVE-2020-8271 para esta vulnerabilidad.
- Un atacante, que pueda comunicarse con la dirección IP / FQDN de SD-WAN Center, podría realizar una omisión de autenticación que diese como resultado la exposición de la funcionalidad SD-WAN. Se ha asignado el identificador CVE-2020-8272 para esta vulnerabilidad.
- Un atacante autenticado en SD-WAN Center podría realizar una escalada de privilegios de un usuario autenticado a *root*. Se ha asignado el identificador CVE-2020-8273 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Limitación incorrecta de una ruta a un directorio restringido en Cisco Security Manager

Fecha de publicación: 17/11/2020

Importancia: Crítica

Recursos afectados:

Cisco Security Manager, versión 4.21 y anteriores.

Descripción:

Florian Hauser ha reportado esta vulnerabilidad al fabricante, de severidad crítica, de tipo limitación incorrecta de una ruta a un directorio restringido (*path traversal*).

Solución:

El fabricante ha publicado la versión 4.22 del producto afectado para solucionar esta vulnerabilidad.

Detalle:

La vulnerabilidad, causada por una validación incorrecta de las secuencias de caracteres transversales de directorio dentro de las solicitudes a un dispositivo afectado, podría permitir a un usuario remoto, no autenticado, enviar un paquete, especialmente diseñado, al dispositivo afectado y, de esta manera, obtener acceso a información sensible o descargar archivos arbitrarios. Se ha asignado el identificador CVE-2020-27130 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 19/11/2020

Importancia: Crítica

Recursos afectados:

- Cisco IoT FND, versiones anteriores a 4.6.1;
- Cisco DNA Spaces Connector, versión 2.2 y anteriores;
- los siguientes productos de Cisco si están ejecutando una versión vulnerable de Cisco IMC:
  - 5000 Series Enterprise Network Compute System (ENCS) Platforms;
  - UCS C-Series Rack Servers, en modo *standalone*;
  - UCS E-Series Servers;
  - UCS S-Series Servers, en modo *standalone*.

Descripción:

Nikita Abramov, investigador de Positive Technologies, junto con diversas pruebas de seguridad interna, han reportado 3 vulnerabilidades, todas de severidad crítica, de falta de autenticación para función crítica, inyección de comandos del sistema operativo y restricción incorrecta de operaciones dentro de los límites de un búfer de memoria.

Solución:

Actualizar los productos afectados a las siguientes versiones:

- Cisco IoT FND, versión 4.6.1 y posteriores;
- Cisco DNA Spaces Connector, versión 2.3 y posteriores;
- para la vulnerabilidad CVE-2020-3470, consultar las tablas de la sección *Fixed Releases*.

Detalle:

- Una vulnerabilidad en la API REST de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto, no autenticado, accediese a la base de datos del *backend*, al obtener un *token* CSRF (*Cross-Site Request Forgery*) y usarlo en las peticiones de la API REST, lo que le permitiría leer, alterar o eliminar información. Se ha asignado el identificador CVE-2020-3531 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz de administración basada en la web de Cisco DNA Spaces Connector podría permitir que un atacante remoto, no autenticado, ejecutase comandos arbitrarios en un dispositivo afectado, mediante el envío de peticiones HTTP especialmente diseñadas. Se ha asignado el identificador CVE-2020-3586 para esta vulnerabilidad.
- Varias vulnerabilidades en el subsistema API de Cisco Integrated Management Controller (IMC) podrían permitir que un atacante remoto, no autenticado, ejecutase código arbitrario con privilegios de *root*, al enviar una solicitud HTTP, especialmente diseñada, al subsistema API. Se ha asignado el identificador CVE-2020-3470 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Comunicaciones, IoT, Vulnerabilidad

---

Vulnerabilidad en el core de Drupal

Fecha de publicación: 19/11/2020

Importancia: Crítica

Recursos afectados:

Versiones anteriores a:

- 9.0.8;
- 8.9.9;
- 8.8.11;
- 7.74.

Descripción: Se ha publicado una vulnerabilidad, de severidad crítica, de tipo ejecución remota de código (RCE), que afecta al *core* de Drupal.

Solución:

Actualizar a las versiones 9.0.8, 8.9.9, 8.8.11 o 7.74.

Las versiones de Drupal 8, anteriores a 8.8.x, están al final de su vida útil y ya no reciben cobertura de seguridad.

Además, es recomendable auditar todos los archivos cargados anteriormente para verificar si hay extensiones maliciosas. Concretamente, archivos que incluyan más de una extensión, como nombre de archivo.php.txt o nombre de archivo.html.gif, sin un guión bajo (_) en la extensión. Las siguientes extensiones de archivo deben considerarse peligrosas, incluso cuando van seguidas de una o más extensiones adicionales:

- phar,
- php,
- pl,
- py,
- cgi,
- asp,
- js,
- html,
- htm,
- phtml.

Este listado no es exhaustivo, por lo que es conveniente evaluar la seguridad de otras extensiones no mencionadas.

Detalle:

El saneado inadecuado de ciertos nombres de archivo en los archivos cargados, podría provocar que los archivos se interpreten como la extensión incorrecta y sirvan como el tipo MIME incorrecto o se ejecuten como PHP para configuraciones de *host* concretas. Se ha asignado el identificador CVE-2020-13671 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 20/11/2020

Importancia: Crítica

Recursos afectados:

- VMware ESXi,
- VMware Workstation Pro / Player (Workstation),
- VMware Fusion Pro / Fusion (Fusion),
- VMware Cloud Foundation.

Descripción:

VMware ha publicado dos vulnerabilidades, de severidades crítica y alta, de uso de la memoria previamente liberada y de escalada de privilegios.

Solución:

Actualizar a alguna de las siguientes versiones y, como medida de mitigación adicional, desactivar el controlador XHCI (USB 3.x).

- Para ESXi 7.0:
  - ESXi70U1b-17168206;
- Para ESXi 6.7:
  - ESXi670-202011101-SG;
- Para ESXi 6.5:
  - ESXi650-202011301-SG;
- Para Fusion 11.x:
  - 11.5.7;
- Para Workstation 15.x:
  - 15.5.7;
- Para VMware Cloud Foundation (ESXi) 4.x:
  - Actualización pendiente;
- Para VMware Cloud Foundation (ESXi) 3.x:
  - Actualización pendiente.

Detalle:

- La vulnerabilidad de uso de la memoria previamente liberada en el controlador XHCI USB, podría permitir a un atacante, con privilegios locales de administrador en una máquina virtual, ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host. Se ha asignado el identificador CVE-2020-4004 para esta vulnerabilidad.
- La gestión inadecuada de las llamadas al sistema, podría permitir a un atacante, con privilegios en el proceso VMX, la escalada de privilegios en el sistema afectado. Esto solo es posible cuando se explota conjuntamente con otra vulnerabilidad, por ejemplo, con la CVE-2020-4004. Se ha asignado el identificador CVE-2020-4005 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad

---

Vulnerabilidad de inyección de comandos en múltiples productos de VMware

Fecha de publicación: 24/11/2020

Importancia: Crítica

Recursos afectados:

- VMware Workspace One Access, versiones 20.01 y 20.10 en Linux;
- VMware Identity Manager, versiones 3.3.1, 3.3.2 y 3.3.3 en Linux;
- VMware Identity Manager Connector, versiones:
  - 3.3.2 y 3.3.1 en Linux;
  - 3.3.3, 3.3.2 y 3.3.1 en Windows.

Descripción:

VMware ha sido informado, de forma privada, sobre una vulnerabilidad crítica de inyección de comandos que afecta a múltiples productos del fabricante.

Solución:

Aplicar las medidas de *workaround* descritas en la sección *Solution* del artículo 81731 publicado por VMware.

Detalle:

Diversos productos de VMware contienen una vulnerabilidad de inyección de comandos en el configurador administrativo. Un atacante, con acceso de red al panel de configuración, en el puerto 8443 y una contraseña válida para la cuenta de administrador de dicho panel, podría ejecutar comandos con privilegios no restringidos en el sistema operativo subyacente. Se ha asignado el identificador CVE-2020-4006 para esta vulnerabilidad.

Etiquetas: Virtualización, VMware, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.23

Fecha de publicación: 25/11/2020

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones:

- desde la 3.0.0, hasta la 3.9.22;
- desde la 2.5.0, hasta la 3.9.22;
- desde la 1.7.0, hasta la 3.9.22.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 7 vulnerabilidades de criticidad baja en su núcleo, de los tipos divulgación de información, limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*),inyección SQL, enumeración de usuarios, *Cross-site Request Forgery* (CSRF) y violación ACL (*Access Control List*).

Solución:

Actualizar a la versión 3.9.23.

Detalle:

- La función *autosuggestion* de *com_finder* ignora el nivel de acceso, lo que podría permitir la divulgación de información.
- La página de configuración global no elimina la información confidencial en la salida HTML, revelando los valores actuales.
- El parámetro de carpeta de *mod_random_image* carece de validación de entrada, lo que podría permitir una limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*).
- El filtrado inadecuado en la configuración de la *blacklist*, podría permitir a un atacante la inyección SQL en la lista de usuarios del *backend*.
- La gestión inadecuada del nombre de usuario, podría permitir a un atacante la enumeración de usuarios en la página de inicio de sesión del *backend*.
- La falta de comprobación del *token* en la función *emailexport* de *com_privacy*, podría permitir a un atacante llevar a cabo ataques de tipo *Cross-site Request Forgery* (CSRF).
- La falta de validación de los datos de entrada durante el uso del conjunto de las reglas ACL, podría permitir a un atacante violar la escritura de ACL.

Etiquetas: Actualización, CMS, Vulnerabilidad

Ejecución arbitraria de código PHP en el core de Drupal

Fecha de publicación: 26/11/2020

Importancia: Alta

Recursos afectados:

Versiones anteriores a:

- 9.0.9;
- 8.9.10;
- 8.8.12;
- 7.75.

Descripción:

Se ha publicado una vulnerabilidad, de severidad crítica, de tipo ejecución arbitraria de código PHP, que afecta al *core* de Drupal.

Solución:

Actualizar a las versiones 9.0.9, 8.9.10, 8.8.12 o 7.75.

Las versiones de Drupal 8, anteriores a 8.8.x, están al final de su vida útil y ya no reciben cobertura de seguridad.

Para mitigar este problema, evite que los usuarios que no sean de confianza, carguen archivos *.tar*; *.tar.gz*; *.bz2* o *.tlz*.

Se recomienda actualizar lo antes posible, ya que existen detalles técnicos que permiten la explotación de esta vulnerabilidad.

Detalle:

La biblioteca *PEAR Archive_Tar*, utilizada por Drupal, ha publicado una actualización de seguridad para solucionar las siguientes vulnerabilidades:

- *Archive_Tar*, versiones anteriores a la 1.4.10, permite un ataque de no serialización porque *"phar:"* está bloqueado, pero *"PHAR:"* no lo está. Se ha asignado el identificador CVE-2020-28948 para esta vulnerabilidad.
- *rchive_Tar*, versiones anteriores a la 1.4.10, presenta una desinfección del nombre de archivo "://" solo para abordar los ataques *phar* y, por lo tanto, cualquier otro ataque de empaquetado de flujo (como "file://" para sobrescribir archivos) aún podría tener éxito. Se ha asignado el identificador CVE-2020-28949 para esta vulnerabilidad.

Los proyectos Drupal que estén configurados para permitir la carga y procesado de archivos *.tar*; *.tar.gz*; *.bz2* o *.tlz*, son vulnerables, además, existen detalles técnicos que permiten la explotación de esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad