Boletín de febrero de 2021

Avisos Técnicos

Limitación inadecuada a directorio restringido en HPE Moonshot Provisioning Manager

Fecha de publicación: 03/02/2021

Importancia: Crítica

Recursos afectados:

HPE Moonshot Provisioning Manager, versión 1.20.

Descripción:

Erik de Jong, en colaboración con ZDI de Trend Micro, ha reportado una vulnerabilidad a HPE, de severidad crítica, de tipo limitación inadecuada a directorio restringido (*directory traversal*).

Solución:

HPE recomienda que los clientes dejen de utilizar HPE Moonshot Provisioning Manager. La aplicación HPE Moonshot Provisioning Manager está descatalogada, ya no recibe soporte, no está disponible para su descarga en el Centro de soporte de HPE y no hay ningún parche disponible.

Detalle:

La vulnerabilidad podría ser explotada por un usuario remoto, no autenticado, para generar una limitación inadecuada a directorio restringido (*directory traversal*) en la entrada suministrada por el usuario al *khuploadfile.cgi*, al no existir suficiente seguridad en cuanto a la validación del usuario, permitiéndole acceder a cualquier tipo de directorio superior sin ningún control, lo que podría provocar la ejecución remota de código, la denegación de servicio y/o comprometer la integridad del sistema. Se ha asignado el identificador CVE-2021-25140 para esta vulnerabilidad.

Etiquetas: HP, Vulnerabilidad

Inyección de código en productos IBM Spectrum Protect

Fecha de publicación: 03/02/2021

Importancia: Crítica

Recursos afectados:

- IBM Spectrum Protect para Virtual Environments: Data Protection para VMware, versiones 8.1.0.0-8.1.10.0 y 7.1.0.0-7.1.8.9;
- IBM Spectrum Protect para Virtual Environments: Data Protection para Hyper-V, versiones 8.1.0.0-8.1.10.0;
- IBM Spectrum Protect Snapshot para VMware, versiones 4.1.0.0-4.1.6.10.

Descripción:

La validación inadecuada de los datos previa a la exportación, en productos IBM Spectrum Protect, podría permitir a un atacante ejecutar código arbitrario en el sistema.

Solución:

- IBM Spectrum Protect para Virtual Environments: Data Protection para VMware Release:
  - versión 8.1: actualizar a la versión 8.1.11;
  - versión 7.1: actualizar a la versión 7.1.8.10.
- IBM Spectrum Protect para Virtual Environments: Data Protection para Hyper-V Release:
  - versión 8.1: actualizar a la versión 8.1.11;
- IBM Spectrum Protect Snapshot para VMware Release:
  - versión 4.1: actualizar a la versión 4.1.6.11.

Detalle:

La validación inadecuada de los datos previa a la exportación en los productos afectados podría permitir a un atacante ejecutar código arbitrario en el sistema. Se ha asignado el identificador CVE-2020-4693 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Denegación de servicio en Flex IO 1794-AENT/B de Allen-Bradley

Fecha de publicación: 03/02/2021

Importancia: Alta

Recursos afectados:

Flex IO 1794-AENT/B, versión 4.003.

Descripción:

El investigador, Jared Rittle, de Cisco Talos, ha informado de una vulnerabilidad de severidad alta que podría permitir a un atacante causar una condición de denegación de servicio (DoS).

Solución:

Actualmente, no existe ninguna actualización disponible.

Detalle:

Una vulnerabilidad de desbordamiento de búfer, en la funcionalidad del segmento de red de la ruta de solicitud ENIP, podría permitir a un atacante la denegación del servicio mediante el envío de una solicitud de red especialmente diseñada. Se ha asignado el identificador CVE- 2020-6088 para esta vulnerabilidad.

Etiquetas: 0day, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Cisco Small Business VPN Routers

Fecha de publicación: 04/02/2021

Importancia: Crítica

Recursos afectados:

Estas vulnerabilidades afectan a los siguientes *routers* Cisco Small Business si ejecutan una versión de *firmware* anterior a la versión 1.0.01.02:

- RV160 VPN Router,
- RV160W Wireless-AC VPN Router,
- RV260 VPN Router,
- RV260P VPN Router con POE,
- RV260W Wireless-AC VPN Router.

Descripción:

Diversos investigadores han notificado a Cisco 7 vulnerabilidades, todas de severidad crítica, que afectan a la interfaz web de gestión de los productos afectados.

Solución:

Cisco ha corregido estas vulnerabilidades en las versiones de *firmware* 1.0.01.02 y posteriores para los *routers* Cisco RV160, RV160W, RV260, RV260P y RV260W, disponibles en el panel de descarga de *software* de Cisco.

Detalle:

La validación incorrecta de peticiones HTTP podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario como *root* en el dispositivo afectado, mediante el envío de peticiones HTTP, especialmente diseñadas, a la interfaz de administración web. Se han asignado los identificadores CVE-2021-1289, CVE-2021-1290, CVE-2021-1291, CVE-2021-1292, CVE-2021-1293, CVE-2021-1294 y CVE-2021-1295 para estas vulnerabilidades.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en SolarWinds Orion Platform

Fecha de publicación: 05/02/2021

Importancia: Crítica

Recursos afectados:

- Orion Platform, versiones anteriores a 2020.2.4;
- ServU-FTP, versiones anteriores a 15.2.2 Hotfix 1.

Descripción:

Martin Rakhmanov, investigador de Trustwave, ha publicado un artículo en el que detalla 3 vulnerabilidades críticas que afectan a SolarWinds Orion User Device Tracker y SolarWinds Serv-U FTP. Estas vulnerabilidades podrían permitir a un atacante la ejecución remota de código, el acceso a las credenciales para su recuperación y la capacidad de leer, escribir o eliminar cualquier archivo del sistema.

Solución:

Las correcciones están disponibles en las siguientes versiones de los productos SolarWinds:

- Orion Platform 2020.2.4;
- ServU-FTP 15.2.2 Hotfix 1.

Detalle:

- El servicio SolarWinds Orion Collector depende en gran medida de MSMQ (*Microsoft Message Queue*), con una gran lista de colas privadas disponibles, todas ellas sin autentificar. Esto significa que los usuarios no autentificados pueden enviar mensajes a las colas a través del puerto TCP 1801. Debido a una deserialización insegura, un usuario sin privilegios podría ejecutar código arbitrario de forma remota. Se ha asignado el identificador CVE-2021-25274 para esta vulnerabilidad.
- Las credenciales de la base de datos del *backend* de Orion no estaban suficientemente protegidas y los usuarios locales tenían acceso sin restricciones a ellas. Un atacante podría aprovechar esta situación para controlar la base de datos de SolarWinds Orion y robar información o añadir usuarios a nivel de administrador. Se ha asignado el identificador CVE-2021-25275 para esta vulnerabilidad.
- Las cuentas ubicadas en SolarWinds Serv-U FTP Server se almacenan en archivos separados en el disco y un usuario autenticado tiene acceso a ellas. El servidor FTP se ejecuta con permisos de *LocalSystem*, por lo que al crear una cuenta de administrador, un atacante podría establecer el directorio de inicio en la raíz de la unidad del sistema y así poder leer o reemplazar cualquier archivo allí. Se ha asignado el identificador CVE-2021-25276 para esta vulnerabilidad.

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

Múltiples vulnerabilidades en Dell PowerScale OneFS

Fecha de publicación: 09/02/2021

Importancia: Crítica

Recursos afectados:

Dell PowerScale OneFS, versiones:

- 8.1.0;
- 8.1.1;
- 8.1.2;
- 8.2.0;
- 8.2.1;
- 8.2.2;
- 9.0.0;
- 9.1.0

Descripción:

Dell EMC ha detectado 7 vulnerabilidades, 1 con severidad crítica, 4 altas y 2 medias, que podrían ser explotados por atacantes para comprometer PowerScale OneFS.

Solución:

Desde la sección de descargas de PowerScale, tomar las acciones concretas descritas en el apartado *Affected Products and Remediation* del aviso del fabricante para cada versión afectada.

Detalle:

Dell PowerScale OneFS contiene una vulnerabilidad de uso de clave SSH después de la expiración de la cuenta. Un usuario en la red, con privilegio RBAC (*Role-Based Access Control*) en *ISI_PRIV_AUTH_SSH*, que tenga una cuenta caducada, podría explotar esta vulnerabilidad, otorgando acceso a lo que tenía antes de la caducidad de la cuenta, existiendo el riesgo de que la cuenta contase con alto nivel de privilegios. Se ha asignado el identificador CVE-2021-21502 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades, se han asignado los identificadores: CVE-2020-26191, CVE-2020-26192, CVE-2020-26195, CVE-2020-26194, CVE-2020-26195 y CVE-2020-26196.

Etiquetas: Actualización, Vulnerabilidad

Actualizaciones de seguridad de Microsoft de febrero de 2021

Fecha de publicación: 10/02/2021

Importancia: Crítica

Recursos afectados:

- .NET Core;
- .NET Framework;
- Azure IoT;
- Developer Tools;
- Microsoft Azure Kubernetes Service;
- Microsoft Dynamics;
- Microsoft Edge para Android;
- Microsoft Exchange Server;
- Microsoft Graphics Component;
- Microsoft Office Excel;
- Microsoft Office SharePoint;
- Microsoft Windows Codecs Library;
- Role: DNS Server;
- Role: Hyper-V;
- Role: Windows Fax Service;
- Skype para Business;
- SysInternals;
- System Center;
- Visual Studio;
- Windows Address Book;
- Windows Backup Engine;
- Windows Console Driver;
- Windows Defender;
- Windows DirectX;
- Windows Event Tracing;
- Windows Installer;
- Windows Kernel;
- Windows Mobile Device Management;
- Windows Network File System;
- Windows PFX Encryption;
- Windows PKU2U;
- Windows PowerShell;
- Windows Print Spooler Components;
- Windows Remote Procedure Call;
- Windows TCP/IP;
- Windows Trust Verification API.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de febrero, consta de 65 vulnerabilidades, 11 clasificadas como críticas, 45 como importantes, 2 moderadas y 7 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 características de seguridad,
- suplantación de identidad (*spoofing*).

IMPORTANTE

- Microsoft ha publicado un aviso de seguridad para solucionar una vulnerabilidad, con severidad alta, de escalada de privilegios en Microsoft Win32k, con identificador CVE-2021-1732. Un atacante local podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado. Esta vulnerabilidad se está explotando actualmente.

- Microsoft ha publicado un post alertando sobre 3 vulnerabilidades existentes en la implementación de TCP/IP de Windows que podrían ser explotadas, de manera remota, por atacantes no autenticados. Las 2 primeras, ambas con severidad crítica, permitirían la ejecución de código remoto (CVE-2021-24074 y CVE-2021-24094), y la tercera, con severidad alta, permitiría llevar a cabo ataques de denegación de servicio (CVE-2021-24086).

Etiquetas: 0day, Actualización, Comunicaciones, DNS, IoT, Microsoft, Navegador, Privacidad, Vulnerabilidad

---

Actualización de seguridad de SAP de febrero de 2021

Fecha de publicación: 10/02/2021

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5;
- SAP Commerce, versiones 1808, 1811, 1905, 2005 y 2011;
- SAP Business Warehouse, versiones 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755 y 782;
- SAP NetWeaverASABAP (SAP Landscape Transformation - DMIS), versiones 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731 y 2011_1_752, 2020;
- SAP S4 HANA (SAP Landscape Transformation), versiones 101, 102, 103, 104 y 105;
- SAP NetWeaverASABAP, versiones 740, 750, 751, 752, 753, 754 y 755;
- SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1), versión 1.0;
- SAP NetWeaver Process Integration (Java Proxy Runtime), versiones 7.10, 7.11, 7.30, 7.31, 7.40 y 7.50;
- SAP Business Objects Business Intelligence Platform (CMC and BI Launchpad), versiones 410, 420 y 430;
- SAP UI5, versiones 1.38.49, 1.52.49, 1.60.34, 1.71.31, 1.78.18, 1.84.5, 1.85.4 y 1.86.1;
- SAP Web Dynpro ABAP;
- SAP UI, versiones 7.5, 7.51, 7.52, 7.53 y 7.54;
- SAP UI 700, versión 2.0;
- SAP HANA Database, versiones 1.0 y 2.0;
- SAP NetWeaver Master Data Management Server, versiones 710 y 710.750.

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.

Para las vulnerabilidades del tipo *tabnabbing* inverso, es posible aplicar las siguientes medidas de mitigación:

- En HTML:
  - Añadir el atributo *rel* en los enlaces HTML: *< a rel="external" href="https://ourpartner.com" target="_self" rel="noopener noreferrer" >texto< /a >.*
  - Añadir directamente en la cabecera HTTP: *Referrer-Policy: noreferrer.*
  - Además, varios de los principales proveedores de navegadores han empezado a proporcionar un comportamiento implícito de *"rel=noopener"* en caso de utilizar *target="_self".*
- En las versiones de JavaScript, mediante la siguiente función:

```
function openPopup(url, name, options){
// Abrir la ventana emergente y establecer la instrucción de política de apertura y referencia.
var newWin = window.open(null, name, 'noopener,noreferrer,' options);
// Restablecer el enlace del abridor.
newWin.opener = null;
// Ahora carga la url correcta.
newWin.location = url; }
```

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 7 notas de seguridad y 6 actualizaciones de notas anteriores, siendo 3 de severidad crítica, 2 altas y 8 medias.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 1 vulnerabilidad de secuestro del click,
- 1 vulnerabilidad de *Cross Site Scripting*,
- 1 vulnerabilidad de denegación de servicio,
- 3 vulnerabilidades de falta de comprobación de autorización,
- 1 vulnerabilidad de ejecución remota de código,
- 1 vulnerabilidad de *SQL injection*,
- 6 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Un atacante autenticado, con privilegios para editar las reglas *drools* en SAP Commerce Cloud, podría ser capaz de inyectar código malicioso en ellas. Esto permitiría la ejecución remota de código cuando las reglas son ejecutadas, pudiendo comprometer el host subyacente y afectar a la confidencialidad, integridad y disponibilidad de la aplicación. Se ha asignado el identificador CVE-2021-21477 para esta vulnerabilidad.
- Un fallo de tipo *tabnabbing inverso* podría permitir que un documento enlazado, que se abra en una nueva pestaña o ventana del navegador, redirija o reemplace la página original por una página de *phishing* sin ninguna interacción por parte del usuario.

Etiquetas: Actualización, SAP, Vulnerabilidad

Ejecución remota de código en Operations Bridge Manager de Micro Focus

Fecha de publicación: 10/02/2021

Importancia: Crítica

Recursos afectados:

Micro Focus Operations Bridge Manager (OBM), versiones:

- 2020.10 (sólo si la configuración por defecto ha sido modificada);
- 2020.05;
- 2019.11;
- 2019.05;
- 2018.11;
- 2018.05;
- 10.6x;
- 10.1x;
- versiones más antiguas.

Descripción:

Se ha reportado una vulnerabilidad de severidad crítica que podría permitir a una atacante ejecutar código de forma remota.

Solución:

Seguir las indicaciones del fabricante en su página web.

Detalle:

Una vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en un servidor OBM. Se ha asignado el identificador CVE-2021-22504 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Evasión de autenticación en Prisma Cloud Compute de Palo Alto Networks

Fecha de publicación: 11/02/2021

Importancia: Crítica

Recursos afectados:

Prisma Cloud Compute, utilizando la autenticación SAML, las siguientes versiones:

- 19.11 < = actualización 2;
- 20.04 < = actualización 2;
- 20.09 < = actualización 2;
- 20.12 < actualización 1.

Descripción:

Palo Alto Networks ha informado de una vulnerabilidad de severidad crítica que podría permitir a un atacante eludir la autenticación en SAML (*Security Assertion Markup Language*).

Solución:

Actualizar Prisma Cloud Compute a la versión 20.12 ? actualización 1 o a una versión posterior.

Como medida de mitigación, se recomienda desactivar la autenticación SAML.

Detalle:

Una verificación incorrecta de la firma digital en la consola de Prisma Cloud Compute podría permitir a un atacante eludir la validación de la firma durante la autenticación SAML y así, iniciar sesión como cualquier usuario autorizado. Se ha asignado el identificador CVE-2021-3033 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Xen

Fecha de publicación: 17/02/2021

Importancia: Alta

Recursos afectados:

- Todas las versiones Linux 3.2 y anteriores, ejecutándose en modo PV en x86 o ejecutándose en Arm. Las versiones Linux ejecutándose en modo HVM (*Hardware Virtual Machine*) / PVH (*Paravirtualization on Hardware*) no son vulnerables.
- Versiones Linux 2.6.39 y superiores en modo PV. Las versiones Linux ejecutándose en modo HVM / PVH no son vulnerables.
- Versiones Linux 4.18 y superiores.
- Xen versión 4.9 y superiores en sistemas Arm.
- Versiones Linux 3.11 y superiores.

Descripción:

Múltiples vulnerabilidades en Xen podrían permitir a un atacante la denegación de servicio, la escalada de privilegios o la divulgación de información.

Solución:

Aplicar la actualización correspondiente:

- xsa361-linux-1.patch;
- xsa361-linux-2.patch;
- xsa361-linux-3.patch;
- xsa361-linux-4.patch;
- xsa361-linux-5.patch;
- xsa362-linux-1.patch;
- xsa362-linux-2.patch;
- xsa362-linux-3.patch;
- xsa363.patch;
- xsa364.patch;
- xsa365-linux.patch.

Detalle:

- Un controlador *frontend* malicioso o con errores, puede ser capaz de bloquear el controlador de *backend* correspondiente, causando una denegación de servicio. Se han asignado los identificadores CVE-2021-26932, CVE-2021-26931 para estas vulnerabilidades.
- Un controlador *frontend* malicioso o con errores, puede ser capaz de bloquear el controlador de *backend* correspondiente, causando una denegación de servicio en todo el *host*. También podría ser posible la escalada de privilegios y la fuga de información. Se ha asignado el identificador CVE-2021-26930 para esta vulnerabilidad.
- La falta de validación en el modo de asignación del *backend* de los controladores *drm_xen_front* de Linux podría permitir que fuera una configuración válida cuando en realidad no fue diseñada para eso. El uso de esta función podría tener consecuencias desconocidas. Se ha asignado el identificador CVE-2021-26934 para esta vulnerabilidad.
- La limpieza de caché inadecuada, podría permitir a un invitado malintencionado leer datos sensibles de la memoria que anteriormente pertenecía a otro invitado. Se ha asignado el identificador CVE-2021-26933 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 24/02/2021

Importancia: Crítica

Recursos afectados:

- vCenter Server, versiones 6.5, 6.7 y 7.0;
- Cloud Foundation (vCenter Server), versiones 3.x y 4.x;
- ESXi, versiones 6.5, 6.7 y 7.0;
- Cloud Foundation (ESXi), versiones 3.x y 4.x.

Descripción:

Mikhail Klyuchnikov, investigador de Positive Technologies, y Lucas Leong, investigador de Trend Micro, han reportado 3 vulnerabilidades, de severidades crítica, alta y media, de tipos ejecución remota de código, desbordamiento de montículo (*heap*) y SSRF (*Server Side Request Forgery*), respectivamente.

Solución:

Actualizar a las siguientes versiones, según el producto afectado:

- vCenter Server, versiones 6.5 U3n, 6.7 U3l y 7.0 U1c;
- Cloud Foundation (vCenter Server), versiones 3.10.1.2 y 4.2;
- ESXi, versiones ESXi650-202102101-SG, ESXi670-202102401-SG y ESXi70U1c-17325551;
- Cloud Foundation (ESXi), versiones KB82705 y 4.2.

Detalle:

- Un atacante, con acceso de red al puerto 443, podría aprovechar una vulnerabilidad en un *plugin* de vCenter Server para vROPs (VMware vRealize Operations), y ejecutar comandos sin restricción de privilegios en el sistema operativo subyacente que aloja vCenter Server. Se ha asignado el identificador CVE-2021-21972 para esta vulnerabilidad crítica.
- Un atacante situado en el mismo segmento de red que ESXi, y que tenga acceso al puerto 427, podría explotar la

vulnerabilidad de desbordamiento de montículo (*heap) en el servicio OpenSLP, lo que resultaría en una ejecución remota de código. Se ha asignado el identificador CVE-2021-21974 para esta vulnerabilidad alta.*
- Un atacante, con acceso de red al puerto 443, podría explotar una vulnerabilidad SSRF, generada por una validación incorrecta de las URL en un *plugin* de vCenter Server, enviando una solicitud POST a dicho *plugin* que podría causar una divulgación de información. Se ha asignado el identificador CVE-2021-21973 para esta vulnerabilidad media.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 25/02/2021

Importancia: Crítica

Recursos afectados:

- Los siguientes productos de Cisco, si están ejecutando Cisco NX-OS Software versiones 9.3(5) o 9.3(6):
  - Nexus 3000 Series Switches,
  - Nexus 9000 Series Switches en modo NX-OS independiente.
- Cisco Application Services Engine Software, versiones 1.1 (3d) y anteriores.
- Cisco ACI Multi-Site Orchestrator (MSO) ejecutando una versión de software 3.0, solo si se desplegó en un Cisco Application Services Engine.

Descripción:

Se han identificado 4 vulnerabilidades en productos de Cisco, todas ellas de severidad crítica, que podrían permitir a un atacante remoto crear, borrar o modificar archivos aleatorios, obtener acceso privilegiado a información sensible u omitir la autenticación en el dispositivo afectado.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas se pueden descargar desde el panel de descarga de Software de Cisco. Para información más detallada, consulte la sección *Referencias*.

Detalle:

- Un atacante podría explotar esta vulnerabilidad enviando paquetes TCP, especialmente diseñados, a una dirección IP configurada en una interfaz local en el puerto TCP 9075. Una explotación exitosa podría permitir al atacante crear, eliminar o sobrescribir archivos arbitrarios, incluyendo archivos sensibles que están relacionados con la configuración del dispositivo. Se ha asignado el identificador CVE-2021-1361 para esta vulnerabilidad.
- Un atacante podría explotar esta vulnerabilidad enviando peticiones TCP, especialmente diseñadas, a un servicio específico. Una explotación exitosa podría permitir al atacante tener acceso privilegiado para ejecutar *containers* o invocar operaciones a nivel de *host*. Se ha asignado el identificador CVE-2021-1393 para esta vulnerabilidad.
- Un atacante podría explotar esta vulnerabilidad enviando peticiones HTTP, especialmente diseñadas, a la API afectada. Una explotación exitosa podría permitir al atacante conocer información específica del dispositivo, crear archivos de soporte técnico en un volumen aislado y realizar cambios de configuración limitados. Se ha asignado el identificador CVE-2021-1396 para esta vulnerabilidad.
- Un atacante podría explotar esta vulnerabilidad enviando una petición, especialmente diseñada, a la API afectada. Una explotación exitosa podría permitir al atacante recibir un *token* con privilegios de nivel de administrador que podría ser utilizado para autenticarse en la API en los dispositivos MSO y Cisco APIC afectados. Se ha asignado el identificador CVE-2021-1388 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad