Boletín de junio de 2020

Avisos Técnicos

Vulnerabilidad de errores de procesamiento de datos en productos de Cisco

Fecha de publicación: 02/06/2020

Importancia: Alta

Recursos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco NX-OS:

- Nexus 1000 Virtual Edge para VMware vSphere;
- Nexus 1000V Switch para Microsoft Hyper-V y VMware vSphere;
- Nexus 3000, 6000 y 7000 Series Switches;
- Nexus 9000 Series Switches en modo independiente NX-OS;
- Nexus 5500 y 5600 Platform Switches;
- UCS 6200 y 6300 Series Fabric Interconnects.

Descripción:

Yannay Livneh ha reportado una vulnerabilidad, de severidad alta, de tipo errores de procesamiento de datos en múltiples productos de Cisco.

Solución:

Las actualizaciones que corrigen la vulnerabilidad indicada, detalladas en la sección *Fixed Software* del aviso, pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

Una vulnerabilidad en la pila de red del software Cisco NX-OS podría permitir que un atacante remoto, no autenticado, omita ciertos límites de seguridad o cause una condición de denegación de servicio (DoS) en un dispositivo afectado. Se ha reservado el identificador CVE-2020-10136 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en ClearPass Policy Manager de Aruba

Fecha de publicación: 03/06/2020

Importancia: Alta

Recursos afectados:

- Clear Pass Policy Manager 6.9.x, versiones anteriores a la versión 6.9.1;
- Clear Pass Policy Manager 6.8.x, versiones anteriores a la versión 6.8.5-HF;
- Clear Pass Policy Manager 6.7.x, versiones anteriores a la versión 6.7.13-HF.

Descripción:

El investigador, Daniel Jensen, reportó a Aruba tres vulnerabilidades, dos de criticidad alta y otra media, de los tipos ejecución remota de código y evasión de la autenticación.

Solución:

- Actualizar Clear Pass Policy Manager 6.9.x a la versión 6.9.1;
- Actualizar Clear Pass Policy Manager 6.8.x a la versión 6.8.5-HF o 6.8.6;
- Actualizar Clear Pass Policy Manager 6.7.x a la versión 6.7.13-HF.

Detalle:

- La interfaz web presenta una vulnerabilidad de evasión de la autenticación. Un atacante remoto que explotase esta vulnerabilidad podría acceder al sistema operativo subyacente. Se ha reservado el identificador CVE-2020-7115 para esta vulnerabilidad.
- La interfaz web de administración presenta dos vulnerabilidades; una alta y otra media, del tipo ejecución remota de código. Un atacante, previamente autenticado en la interfaz de administración, podría realizar una ejecución remota de código en el sistema operativo subyacente. Se han reservado los identificadores CVE-2020-7116 y CVE-2020-7117 para estas vulnerabilidades.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.19

Fecha de publicación: 03/06/2020

Importancia: Media

Recursos afectados:

- Joomla! CMS, versiones:
  - desde la 2.5.0 hasta la 3.9.18;
  - desde la 3.0.0 hasta la 3.9.18.

Descripción:

Joomla! ha publicado una nueva versión que soluciona 5 vulnerabilidades que afectan a su núcleo. Soluciona una vulnerabilidad de criticidad media y cuatro de criticidad baja, del tipo *Cross-site scripting* (XSS), *Cross-site request forgery* (CSRF) y fallo en las configuraciones por defecto.

Solución:

Actualizar Joomla! a la versión 3.9.19.

Detalle:

- La vulnerabilidad de criticidad media afecta a los métodos de manipulación del DOM de jQuery, pudiendo permitir un ataque XSS. Se han asignado los identificadores CVE-2020-11022 y CVE-2020-11023 para esta vulnerabilidad.
- Las vulnerabilidades de severidad baja están descritas a continuación:
  - Una falta de validación de parámetros de entrada en la opción de los encabezados de las etiquetas de los módulos "Articles ? Newsflash" y "Articles ? Categories", permitirían realizar ataques XSS. Se ha asignado el identificador CVE-2020-13761 para esta vulnerabilidad.
  - Los parámetros por defecto de la configuración global de "textfilter" no bloquean entradas HTML de los usuarios invitados ("Guest"). Se ha asignado el CVE-2020-13763 para esta vulnerabilidad.
  - Una incorrecta validación de entrada en la etiqueta opción del módulo *com_modules* podría permitir ataques XSS. Se ha asignado el identificador CVE-2020-13762 para esta vulnerabilidad.
  - Una falta de comprobación de los tokens en *com_postinstall* podría permitir un ataque del tipo CSRF. Se ha asignado el identificador CVE-2020-13760 para esta vulnerabilidad

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de inyección de comandos del SO en IBM Security Guardium

Fecha de publicación: 03/06/2020

Importancia: Alta

Recursos afectados:

IBM Security Guardium, versión 11.1.

Descripción:

Una vulnerabilidad en IBM Security Guardium podría permitir a un atacante ejecutar comandos arbitrarios en el sistema.

Solución:

Aplicar el parche que soluciona la vulnerabilidad.

Detalle:

La vulnerabilidad podría permitir a un atacante autentificado remotamente ejecutar comandos arbitrarios en el sistema por medio de una solicitud especialmente diseñada. Se ha reservado el identificador CVE-2020-4180 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de inyección XXE en IBM QRadar

Fecha de publicación: 04/06/2020

Importancia: Alta

Recursos afectados:

Todas las versiones del protocolo SDEE (*Security Device Event Exchange*) anteriores a:

- 7.3.0-QRADAR-PROTOCOL-SDEE-7.3-20200429181957;
- 7.4.0-QRADAR-PROTOCOL-SDEE-7.4-20200429181942

Descripción:

Varios componentes de IBM X-Force Ethical Hacking Team han descubierto una vulnerabilidad, de severidad alta, de tipo inyección XXE (*XML External Entity*), que afecta al producto QRadar de IBM.

Solución:

Actualizar el producto afectado a las versiones 7.4.0-QRADAR-PROTOCOL-SDEE-7.4-20200429181942 o 7.3.0-QRADAR-PROTOCOL-SDEE-7.3-20200429181957.

Detalle:

IBM QRadar es vulnerable a un ataque de inyección XXE (*XML External Entity*) al procesar datos XML. Un atacante remoto podría aprovechar esta vulnerabilidad para exponer información confidencial o consumir recursos de memoria. Se ha reservado el identificador CVE-2020-4509 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de evasión de autenticación en GnuTLS

Fecha de publicación: 04/06/2020

Importancia: Alta

Recursos afectados:

GnuTLS, versión 3.6.4.

Descripción:

Se ha publicado una vulnerabilidad en el servidor TLS de GnuTLS que podría permitir a un atacante eludir la autenticación en TLS 1.3 y recuperar las conversaciones anteriores en TLS 1.2.

Solución:

Actualizar a la versión 3.6.14 o posteriores.

Detalle:

Los servidores de GnuTLS son capaces de utilizar los tickets emitidos por cada uno de ellos sin tener acceso a la clave secreta generada por *gnutls_session_ticket_key_generate()*. Esto podría permitir a un atacante MITM, sin credenciales válidas, reanudar las sesiones con un cliente que haya establecido previamente una conexión con un servidor con credenciales válidas. Se ha reservado el identificador CVE-2020-13777 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos de Cisco

Fecha de publicación: 04/06/2020

Importancia: Crítica

Recursos afectados:

- Cisco IOS XE, versión 16.3.1 y anteriores si tienen configurado la aplicación IOx *hosting infrastrucutre*;
- Los siguientes productos Cisco que estén ejecutando una versión vulnerable de Cisco IOS Software:
  - Cisco 809 and 829 Industrial ISRs,
  - CGR1000,
- Cisco IOS;
- Cisco IOS XE;
- Cisco IOS XXR;
- Cisco IOS XE, con la web UI habilitada;
- Cisco IOS XE, con la característica servidor HTTP habilitada;
- Cisco IOS o Cisco IOS XE, configurados para CIP. CIP no viene configurado por defecto;
- Cisco IOS o Cisco IOS XE, configurados para aceptar conexiones SSH;
- Cisco IOS o Cisco IOS XE, con la característica IKEv2 configurada. Los dispositivos con la característica IKEv1 no se encuentran afectados.
- Cisco Catalyst Series Switches, que ejecutan una versión vulnerable de Cisco IOS o Cisco IOS XE:
  - Cisco Catalyst 4500, que estén configurados para SNMP *polling*, y disponga de tarjetas *Power over Ethernet* (PoE) instaladas;
  - Cisco Catalyst 9800, que dispongan de la característica *Aplication Visibility and Control* (AVC) habilitada, o estén configurados con LSCs.
  - Catalyst 3650 Series Switches;
  - Catalyst 3850 Series Switches;
  - Catalyst 9200 Series Switches;
  - Catalyst 9300 Series Switches;

    - Catalyst 9500 Series Switches.
- Routers Cisco, que ejecuten versiones vulnerables de Cisco IOS o Cisco IOS XS, con las siguientes características configuradas:
    - Cisco Unified Border Element (CUBE);
    - Cisco Unified Communications Manager Express (CME);
    - Cisco IOS Gateways con Session Initiation Protocol (SIP)
    - Cisco TDM Gateways;
    - Cisco Unified Survivable Remote Site Telephony (SRST);
    - Cisco Business Edition 4000 (BE4K).
- Los siguientes dispositivos que dispongan de Cisco NX-OS y tengan la característica onePK habilitada:
    - Nexus 3000 Series Switches;
    - Nexus 5500 Platform Switches;
    - Nexus 5600 Platform Switches;
    - Nexus 6000 Series Switches;
    - Nexus 7000 Series Switches;
    - Nexus 9000 Series Switches en modo NX-OS independiente (*standalone*).
- Dispositivos Cisco que ejecuten versiones de Cisco IOx Application Framework anteriores a la 1.9.0:
    - 800 Series Industrial Integrated Services Routers (Industrial ISRs);
    - 800 Series Integrated Services Routers (ISRs);
    - 1000 Series Connected Grid Routers (CGR1000) Compute Module;
    - IC3000 Industrial Compute Gateway;
    - Industrial Ethernet (IE) 4000 Series Switches;
    - Dispositivos basados en IOS XE:
        - 1000 Series ISRs,
        - 4000 Series ISRs,
        - ASR 1000 Series Aggregation Services Routers,
        - Catalyst 9x00 Series Switches,
        - Catalyst IE3400 Rugged Series Switches,
        - Embedded Services 3300 Series Switches,
    - IR510 WPAN Industrial Routers.

Descripción:

Cisco ha detectado 26 vulnerabilidades, 4 de severidad crítica y 22 de severidad alta, que afectan a múltiples productos.

Solución:

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

Detalle:

Las vulnerabilidades detectas podrían permitir a un atacante realizar las siguientes acciones:

- Escalada de privilegios,
- Inyección de comandos,
- Ejecución de código arbitrario,
- Ejecución remota de código con privilegios de *root*,
- Generar una condición de denegación de servicio (DoS),
- Instalación de software no autorizado en el dispositivo,
- Acceder al sistema mediante el uso de credenciales embebidas,
- Manipulación de ficheros.

A las vulnerabilidades de severidad crítica se les han asignado los identificadores CVE-2020-3227, CVE-2020-3205, CVE-2020-3198 y CVE-2020-3198.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de divulgación de información en WebSphere Application Server de IBM

Fecha de publicación: 05/06/2020

Importancia: Alta

Recursos afectados:

WebSphere Application Server, versiones 7.0, 8.0, 8.5 y 9.0.

Descripción:

Se ha publicado una vulnerabilidad en el servidor de aplicaciones WebSphere que podría permitir a un atacante la divulgación de información.

Solución:

- Para las versiones desde la 9.0.0.0, hasta la 9.0.5.4:
    - Aplicar el Interim Fix PH25074 o actualizar a la versión 9.0.5.5 o posterior (disponible en 3Q2020);
- Para las versiones desde la 8.5.0.0, hasta la 8.5.5.17:
    - Aplicar el Interim Fix PH25074 o actualizar a la versión 8.5.5.18 o posterior (disponible en 3Q2020);
- Para las versiones desde la 8.0.0.0, hasta la 8.0.0.15:
    - Actualizar a la versión 8.0.0.15 y posteriormente aplicar el Interim Fix PH25074;
- Para las versiones desde la 7.0.0.0, hasta la 7.0.0.45:
    - Actualizar a la versión 7.0.0.45 y posteriormente aplicar el Interim Fix PH25074;

Detalle:

Una vulnerabilidad en IBM WebSphere Application Server podría permitir a un atacante remoto obtener información sensible con una secuencia especialmente diseñada de objetos serializados. Se ha reservado el identificador CVE-2020-4449 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de SSRF en IBM Maximo Asset Management

Fecha de publicación: 08/06/2020

Importancia: Alta

Recursos afectados:

- IBM Maximo Asset Management, versiones 7.6.0 y 7.6.1;
- productos de soluciones industriales afectados si se utiliza una versión principal afectada:
  - Maximo para aviación,
  - Maximo para ciencias de la vida,
  - Maximo para energía nuclear,
  - Maximo para petróleo y gas,
  - Maximo para transporte,
  - Maximo para servicios públicos;
- productos IBM Control Desk afectados si usan una versión principal afectada:
  - SmartCloud Control Desk,
  - IBM Control Desk,
  - Tivoli Integration Composer.

Descripción:

Los investigadores Andrey Medov y Arseniy Sharoglazov, de Positive Technologies, reportaron a IBM una vulnerabilidad, de severidad alta, de tipo SSRF (*Server Side Request Forgery*) que afecta al producto Maximo Asset Management del fabricante.

Solución:

Desde la versión 7.6.0.4 de IBM Maximo Asset Management, se agregó la función de impresión sin *applet* y una propiedad donde la impresión de *applet* está desactivada de forma predeterminada. Para solucionar esta vulnerabilidad, evitar el uso de la impresión de *applet*.

Detalle:

Esta vulnerabilidad podría permitir que un atacante autenticado envíe solicitudes no autorizadas desde el sistema, lo que podría provocar la enumeración de la red (conseguir información de usuarios, grupos o dispositivos y demás servicios relacionados de una red de ordenadores) o facilitar otros ataques. Se ha reservado el identificador CVE-2020-4529 para esta vulnerabilidad.

Etiquetas: IBM, Vulnerabilidad

Vulnerabilidad en la implementación de UPnP

Fecha de publicación: 09/06/2020

Importancia: Crítica

Recursos afectados:

Protocolo Universal Plug and Play (UPnP), versión anterior al 17 de abril de 2020.

Descripción:

Yunus Çadirci ha reportado una vulnerabilidad en el protocolo Universal Plug and Play (UPnP) que podría permitir el envío de tráfico a destinos arbitrarios usando la funcionalidad *SUBSCRIBE*.

Solución:

- La OCF ha actualizado la especificación UPnP para abordar este problema. Los usuarios deben monitorizar los canales de soporte de los vendedores a la espera de que estos implementen la nueva especificación SUBSCRIBE.
- Se insta a los fabricantes de dispositivos a que deshabiliten la capacidad SUBSCRIBE en su configuración predeterminada y a que exijan a los usuarios que habiliten explícitamente esta función con las restricciones de red apropiadas para limitar su uso a una red de área local de confianza.
- La siguiente regla del IDS de Suricata busca cualquier solicitud de HTTP SUBSCRIBE a una red probablemente externa, es decir, no las direcciones RFC1918, ni RFC4193. Los administradores de red y los proveedores de servicios de Internet pueden desplegar esta firma en el punto de acceso a Internet para detectar cualquier solicitud anómala de SUSCRIPCIÓN que llegue a sus usuarios.
  - alert http any any - > ![fd00::/8,192.168.0.0/16,10.0.0.0/8,172.16.0.0/12] any (msg:"UPnP SUBSCRIBE request seen to external network VU#339275: CVE- 2020-12695 https://kb.cert.org "; content: "subscribe"; nocase; http_met hod; sid:1367339275;)

Detalle:

Una vulnerabilidad en la capacidad de UPnP SUBSCRIBE podría permitir a un atacante remoto, no autenticado, enviar grandes cantidades de datos a destinos arbitrarios accesibles a través de Internet, lo que podría conducir a una denegación de servicio distribuida (DDoS), exfiltración de datos y otros comportamientos inesperados de la red. Se ha asignado el identificador CVE-2020-12695 para esta vulnerabilidad también denominada *Call Stranger*.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Liferay Portal

Fecha de publicación: 09/06/2020

Importancia: Crítica

Recursos afectados:

Liferay Portal, versiones:

- 7.2.1 y anteriores;
- 7.x anteriores a 7.3.2;
- 7.1.3, 7.2.0, 7.2.1 y posiblemente versiones anteriores no compatibles.

Descripción:

Varios investigadores han detectado múltiples vulnerabilidades en el gestor de contenidos Liferay Portal, 4 de severidad crítica (clasificado por el fabricante como *severity 1*) y 11 de severidad alta y media (*severity 2* según el baremo empleado por Liferay). Los tipos de vulnerabilidad son: deserialización en Java, exposición de credenciales LDAP, pérdida de contraseña del proveedor de datos REST, ejecución remota de código, CSRF, SSRF, XSS, MitM, elusión de restricción de extensión de archivos, acceso a directorios no controlado, inyección de correo, falta de comprobación de permisos de usuarios e instancia no configurada de un *widget* instanciable.

Solución:

Actualizar a las siguientes versiones:

- Liferay Portal 7.2 GA2 (7.2.1),
- Liferay Portal 7.1 GA4 (7.1.3),
- no hay parche para Liferay Portal 7.3.1 y anteriores, se debe actualizar directamente a 7.3 CE GA3 (7.3.2) o posteriores;
- no hay parche para Liferay Portal 7.2.0, se debe actualizar directamente a 7.2 CE GA2 (7.2.1) o posteriores.

Detalle:

Un atacante podría realizar las siguientes acciones si aprovechara alguna de las vulnerabilidades enumeradas anteriormente:

- intercepción y modificación de comunicaciones;
- obtención de credenciales LDAP;
- un usuario remoto, autenticado, podría obtener la contraseña de REST Data Providers. Se ha reservado el identificador CVE-2020-13444 para esta vulnerabilidad;
- un usuario remoto, autenticado, podría ejecutar código arbitrario a través de plantillas especialmente diseñadas. Se ha reservado el identificador CVE-2020-13445 para esta vulnerabilidad;
- acceso a información sensible;
- un atacante remoto podría inyectar un *script* web arbitrario o HTML;
- sobreescritura de archivos en el sistema;
- ataque de *phishing*;
- redirigir al usuario a un sitio web externo;
- usuarios autenticados, remotos, podrían consultar grupos de usuarios que pertenecen al sitio web a través del panel de administración de la propia web.

Etiquetas: Actualización, CMS, Vulnerabilidad

Boletín de seguridad de Microsoft de junio de 2020

Fecha de publicación: 10/06/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge (basado en Chromium) en modo IE;
- Microsoft ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Windows Defender;
- Microsoft Dynamics;
- Visual Studio;
- Azure DevOps;
- HoloLens;
- Adobe Flash Player;
- Microsoft Apps para Android;
- Windows App Store;
- System Center;
- Android App.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de junio, consta de 129 vulnerabilidades, 11 clasificadas como críticas y 118 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:

- ejecución remota de código,
- escalada de privilegios,
- denegación de servicio,
- divulgación de información,

- suplantación de identidad (*spoofing*),
- evasión de las restricciones de seguridad.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Vulnerabilidades en Managed File Transfer Platform Server para IBM i de TIBCO

Fecha de publicación: 10/06/2020

Importancia: Crítica

Recursos afectados:

TIBCO Managed File Transfer Platform Server para IBM i, versiones:

- 7.1.0 y anteriores;
- 8.0.0.

Descripción:

TIBCO ha publicado dos vulnerabilidades de severidad crítica del tipo ejecución arbitraria de comandos, revelación de información y manipulación no autorizada de ficheros.

Solución:

Actualizar TIBCO Managed File Transfer Platform Server for IBM i, a las versiones:

- 7.11 o superior;
- 8.0.1 o superior.

Detalle:

Las vulnerabilidades críticas que afectan al componente *file transfer*, son descritas a continuación:

- Un atacante remoto, no autenticado, podría ejecutar comandos arbitrarios con los privilegios del sistema afectado después de una transferencia fallida. Se ha asignado el identificador CVE-2020-9412 para esta vulnerabilidad.
- Cuando la opción de configuración *Require Node Resp* está configurada a *No*. Un atacante remoto, no autenticado, podría acceder a los archivos del sistema y manipularlos, lo que podría afectar a la integridad del sistema operativo subyacente en el dispositivo afectado. Se ha asignado el identificador CVE-2020-9411 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Intel de junio 2020

Fecha de publicación: 10/06/2020

Importancia: Crítica

Recursos afectados:

- Intel Converged Security and Manageability Engine (CSME);
- Intel Server Platform Services (SPS);
- Intel Trusted Execution Engine (TXE);
- Intel Active Management Technology (AMT);
- Intel Standard Manageability (ISM);
- Intel Dynamic Application Loader (DAL);
- Intel SSD, series:
  - D3-S4510;
  - DC P4510;
  - DC P4610;
  - DC P4618;
  - DC P4511;
  - D5-P4326;
  - D5-P4420;
  - D5-P4320.
- Múltiples procesadores de Intel, puede consultar la siguiente lista;
- Firmware de las BIOS de la familia de procesadores Intel Core:
  - 7ª generación;
  - 8ª generación;
  - 9ª generación;
  - 10ª generación.
- Intel Innovation Engine Build y Signing Tool, versiones anteriores a la 1.0.859.

Las vulnerabilidades en los productos de Intel descritos anteriormente afectan a los siguientes fabricantes:

- Citrix/Xen:
  - Citrix Hypervisor 8.0;
  - Citrix Hypervisor 8.1;
  - XenServer 7.0;
  - XenServer 7.1 LTSR Cumulative Update 2.

Descripción:

Varios investigadores y entidades han reportado a Intel 25 vulnerabilidades, de las cuales hay 2 con severidad crítica, 11 altas, 11 medias

y una baja,

Solución:

Intel ha publicado una serie de actualizaciones que solucionan las vulnerabilidades en función del producto y versión afectadas. Para información mas detallada, visite el apartado *Referencias*.

Para los fabricantes afectados por estas vulnerabilidades:

- Citrix / Xen:
  - Citrix Hypervisor 8.1, aplicar el parche CTX272278;
  - Citrix Hypervisor 8.0, aplicar el parche CTX272277;
  - Citrix XenServer 7.1 LTSR CU2, aplicar el parche CTX272276
  - Citrix XenServer 7.0, aplicar el parche CTX272275.

Detalle:

Las vulnerabilidades detectadas podrían permitir a un atacante realizar las siguientes acciones:

- escalada de privilegios,
- generar una condición de denegación de servicio,
- revelado de información.

Destacar la vulnerabilidad con el identificador CVE-2020-0543 denominada CROSSTALK, que podría permitir a un atacante revelar información.

A las vulnerabilidades con severidad crítica se les han reservado los identificadores CVE-2020-0594 y CVE-2020-0595.

A las vulnerabilidades con criticidad alta se les han reservado los identificadores CVE-2020-0586, CVE-2020-0542, CVE-2020-0596, CVE-2020-0538, CVE-2020-0534, CVE-2020-0533, CVE-2020-0532, CVE-2020-0566, CVE-2020-0527, CVE-2020-0528 y CVE-2020-8675.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de junio de 2020

Fecha de publicación: 10/06/2020

Importancia: Crítica

Recursos afectados:

- SAP Liquidity Management for Banking, versión 6.2;
- SAP Commerce, versiones 6.7, 1808, 1811 y 1905;
- SAP Commerce (Data Hub), versiones 6.7, 1808, 1811 y 1905;
- SAP Commerce, versiones 6.7, 1808, 1811 y 1905;
- SAP Solution Manager (Problem Context Manager), versión 7.2;
- SAP SuccessFactors Recruiting, versión 2005;
- SAP Netweaver AS ABAP, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753 y 754;
- SAP NetWeaver AS JAVA (P4 Protocol), versiones:
  - SAP-JEECOR 7.00 y 7.01;
  - SERVERCOR 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
  - CORE-TOOLS 7.00, 7.01, 7.02, 7.05, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver AS ABAP (Banking Services), versiones 710, 711, 740, 750, 751, 752, 75A, 75B, 75C, 75D y 75E;
- SAP Solution Manager (Trace Analysis), versión 7.20;
- Adobe LiveCycle Designer, versión 11.0;
- SAP NetWeaver AS ABAP (Business Server Pages Test Application SBSPEXT_TABLE), versiones 700, 701, 702, 730, 731, 740, 750, 751, 752, 753 y 754;
- SAP Fiori for SAP S/4HANA, versiones 200, 300, 400 y 500;
- SAP ERP (Statutory Reporting for Insurance Companies), versiones EA-FINSERV 600, 603, 604, 605, 606, 616, 617, 618 y 800, y S4CORE 101, 102, 103 y 104;
- SAP Business One(Backup service), versiones 9.3 y 10.0;
- SAP Gateway, versiones 7.40, 2.00, 7.5, 7.51, 7.52 y 7.53;
- SAP Business Objects Business Intelligence Platform, versión 4.2.

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.
- El parche proporcionado para la vulnerabilidad CVE-2020-6265 sólo afecta a las nuevas instalaciones de SAP Commerce (Data Hub), no elimina las contraseñas predeterminadas de las cuentas incorporadas de las instalaciones existentes, por lo que el fabricante propone reiniciar la instalación de SAP Commerce después de aplicar el parche.
- Para la vulnerabilidad CVE-2020-1938, debido a una conocida vulnerabilidad en Apache Tomcat, llamada *Ghostcat*, SAP recomienda encarecidamente desactivar todos los puertos que utilizan el protocolo Apache JServ (Protocolo AJP). Si los clientes necesitan este protocolo se recomienda establecer el atributo secreto requerido en la configuración del conector AJP.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 17 notas de seguridad y 1 actualización, siendo 2 de ellas de severidad crítica, 4 altas y 12 medias.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 1 vulnerabilidad de *Cross-Site Scripting*,
- 1 vulnerabilidad de credenciales embebidas,
- 3 vulnerabilidades de divulgación de información,
- 1 vulnerabilidad de falta de autenticación,
- 3 vulnerabilidades de falta de comprobación de autenticación,

- 3 vulnerabilidades de de falta devalidación de XML,
- 2 vulnerabilidades de redirección de URL,
- 6 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Los productos SAP Commerce and SAP Commerce Data Hub utilizan algunas cuentas de usuario con contraseñas conocidas públicamente y no obligan a los administradores a cambiar estas contraseñas durante o después de la instalación de la aplicación. Se ha reservado el identificador CVE-2020-6265 para esta vulnerabilidad.
- Las conexiones AJP pueden ser explotadas permitiendo a un atacante la ejecución remota de código y otras operaciones. Se ha asignado el identificador CVE-2020-1938 para esta vulnerabilidad.
- Bajo una configuración específica de algunas propiedades, un atacante podría explotar características inseguras en el formulario de inicio de sesión para obtener información que podría ser utilizada para otros exploits y ataques futuros. Algunas de estas propiedades requeridas están incluso configurados por defecto. Se ha reservado el CVE-2020-6264 para esta vulnerabilidad.

Etiquetas: Actualización, SAP, Vulnerabilidad

Escalada de privilegios en VMware Horizon Client

Fecha de publicación: 11/06/2020

Importancia: Alta

Recursos afectados:

VMware Horizon Client para Windows, versiones anteriores a 5.4.3.

Descripción:

Se ha publicado una vulnerabilidad de escalada de privilegios en VMware Horizon Client para Windows.

Solución:

Actualizar a la versión 5.4.3.

Detalle:

VMware Horizon Client for Windows contiene una vulnerabilidad de escalada de privilegios debido a la configuración de permisos de carpeta y a la carga insegura de las bibliotecas. Se ha reservado el identificador CVE-2020-3961 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Actualización de seguridad 5.4.2 para WordPress

Fecha de publicación: 11/06/2020

Importancia: Alta

Recursos afectados:

WordPress, versiones 5.4.1 y anteriores.

Descripción:

Se ha publicado la última versión de WordPress, que corrige 6 problemas de seguridad.

Solución:

Actualizar a la versión 5.4.2.

Detalle:

Las correcciones de seguridad solucionan las siguientes vulnerabilidades, que podrían permitir a un atacante:

- realizar XSS (*Cross-Site Scripting*),
- redirección abierta en *wp_validate_redirect()*,
- escalada de privilegios a través de un uso incorrecto de *set-screen-option*,
- mostrar comentarios y contraseñas protegidas bajo ciertas condiciones.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos Paloalto

Fecha de publicación: 11/06/2020

Importancia: Alta

Recursos afectados:

- PAN-OS:
  - versiones 9.0 anteriores a la 9.0.7;
  - versiones 8.1 anteriores a la 8.1.13;
  - todas las versiones 8.0;

    - todas las versiones 7.1;
- GlobalProtect App:
    - versiones 5.1 para windows anteriores a la 5.1.4
    - versiones 5.0 para windows anteriores a la 5.0.10

Descripción:

Se han publicado múltiples vulnerabilidades en productos Paloalto que podrían permitir a un atacante interrumpir los procesos del sistema y ejecutar código arbitrario con privilegios de root, ejecutar comandos arbitrarios del SO con privilegios de root o ejecutar programas con privilegios SYSTEM.

Solución:

Actualizar a:

- PAN-OS:
    - versión 9.0.7;
    - versión 8.1.13;
    - las versiones 8.0 se encuentran en fin de soporte y no recibirán ninguna actualización;
    - las versiones 7.1 solo recibirán actualizaciones para las vulnerabilidades críticas;
- GlobalProtect App:
    - versiones 5.1.4 o superiores;
    - versiones 5.0.10 o superiores.

Detalle:

- Una vulnerabilidad de desbordamiento de búfer en el componente authd del servidor de gestión de PAN-OS podría permitir a los administradores autentificados interrumpir los procesos del sistema y ejecutar código arbitrario con privilegios de root. Se ha asignado el identificador CVE-2020-2027 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de comandos del SO en el servidor de administración de PAN-OS permite a los administradores autentificados ejecutar comandos arbitrarios del SO con privilegios de root al subir un nuevo certificado en el modo FIPS-CC. Se ha asignado el identificador CVE-2020-2028 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de comandos del SO en la interfaz de administración web de PAN-OS permite a los administradores autentificados ejecutar comandos arbitrarios del SO con privilegios de root enviando una solicitud maliciosa para generar nuevos certificados para su uso en la configuración de PAN-OS. Se ha asignado el identificador CVE-2020-2029 para esta vulnerabilidad.
- Una vulnerabilidad de condición de carrera en GlobalProtect, en Windows, permite a un usuario local ejecutar programas con privilegios SYSTEM. Este problema sólo puede ser explotado mientras se realiza una actualización de la aplicación GlobalProtect. Se ha asignado el identificador CVE-2020-2032 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de Citrix

Fecha de publicación: 12/06/2020

Importancia: Alta

Recursos afectados:

- Citrix Receiver para Windows, todas las versiones;
- Citrix Workspace App, versiones anteriores a la 1912.

Descripción:

El investigador Andrew Hess ha detectado dos vulnerabilidades, ambas con severidad alta, de tipo permisos predeterminados incorrectos.

Solución:

Los usuarios de ambos productos afectados deben actualizar Citrix Workspace App a la versión 1912 o posteriores, incluidas las versiones LTSR.

Detalle:

Un usuario local podría escalar privilegios, hasta llegar a ser administrador, durante el proceso de desinstalación de los productos afectados. Se han asignado los identificadores CVE-2020-13884 y CVE-2020-13885 para estas vulnerabilidades.

Etiquetas: Actualización, Virtualización, Vulnerabilidad

Múltiples vulnerabilidades en productos IBM

Fecha de publicación: 15/06/2020

Importancia: Alta

Recursos afectados:

IBM Spectrum Protect Plus, versiones 10.1.0 - 10.1.5.

Descripción:

Se han publicado múltiples vulnerabilidades en productos IBM que podrían permitir a un atacante la ejecución remota de código, la denegación de servicio, la omisión de autenticación o el secuestro de sesiones de DNS.

Solución:

Actualizar a IBM Spectrum Protect Plus, versión 10.1.6.

Detalle:

- IBM Spectrum Protect Plus podría permitir a un atacante remoto ejecutar un código arbitrario en el sistema mediante el uso de un comando HTTP especialmente diseñado. Se ha asignado el identificador CVE-2020-4469 para esta vulnerabilidad.
- IBM Spectrum Protect Plus podría permitir a un atacante no autenticado causar una denegación de servicio o secuestrar sesiones de DNS enviando un comando HTTP, especialmente diseñado, al servidor remoto. Se ha reservado el identificador CVE-2020-4471 para esta vulnerabilidad.
- La Consola Administrativa de IBM Spectrum Protect Plus podría permitir a un atacante autentificado subir archivos arbitrarios para ejecutar código arbitrario en el servidor vulnerable. Se ha reservado el identificador CVE-2020-4470 para esta vulnerabilidad.
- IBM Spectrum Protect Plus contiene credenciales codificadas, como una contraseña o clave criptográfica, que utiliza para su propia autenticación de entrada, comunicación de salida a componentes externos o cifrado de datos internos. Se ha reservado el identificador CVE-2020-4216 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 17/06/2020

Importancia: Crítica

Recursos afectados:

Cuando se ejecutan las versiones de *firmware* anteriores a 3.2.15.25, en los siguientes productos:

- RBK752,
- RBK753,
- RBK753S,
- RBR750,
- RBS750,
- RBK852,
- RBK853,
- RBR850,
- RBS850,
- RBK842,
- RBR840,
- RBS840.

Descripción:

Netgear ha publicado 15 vulnerabilidades, 12 de severidad crítica y 3 de severidad alta, que afectan a sus productos.

Solución:

Acceder a la página de soporte de Netgear, y descargar la última versión del *firmware* del dispositivo afectado.

Detalle:

Los tipos de vulnerabildiades descritos en el conjunto de avisos publicados por Netgear son:

- divulgación de credenciales de administrador,
- inyección de comandos después de la autenticación,
- inyección de comandos antes de la autenticación,
- CSRF (*Cross Site Request Forgery*).

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 18/06/2020

Importancia: Alta

Recursos afectados:

- Cisco Webex Meetings, versiones:
  - WBS 39.5.25 y anteriores;
  - WBS 40.4.10 y anteriores;
  - WBS 40.6.0.
- Cisco Webex Meetings Server, versiones 4.0MR3 y anteriores;
- Cisco Webex Meetings Desktop App, versiones anteriores a 39.5.12;
- Cisco Webex Meetings Desktop App para Mac, versiones anteriores a 39.5.11;
- Cisco TelePresence Collaboration Endpoint Software y RoomOS Software, versiones anteriores a May Drop 2 2020;
- Cisco Small Business, versiones de routers y *firmware*:
  - RV016 Multi-WAN VPN 4.2.3.10 y anteriores;
  - RV042 Dual WAN VPN 4.2.3.10 y anteriores;
  - RV042G Dual Gigabit WAN VPN 4.2.3.10 y anteriores;
  - RV082 Dual WAN VPN 4.2.3.10 y anteriores;
  - RV320 Dual Gigabit WAN VPN 1.5.1.05 y anteriores;
  - RV325 Dual Gigabit WAN VPN 1.5.1.05 y anteriores;
  - RV110W Wireless-N VPN Firewall 1.2.2.5 y anteriores;
  - RV130 VPN Router 1.0.3.54 y anteriores;
  - RV130W Wireless-N Multifunction VPN Router 1.0.3.54 y anteriores;
  - RV215W Wireless-N VPN Router 1.3.1.5 y anteriores.

Descripción:

Cisco ha detectado 23 vulnerabilidades de severidad alta que afectan a múltiples productos.

Solución:

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

Detalle:

Las vulnerabilidades detectadas podrían permitir a un atacante remoto realizar las siguientes acciones:

- obtener acceso no autorizado a un sitio Webex vulnerable,
- ejecutar programas en el sistema de usuario final,
- ejecutar código arbitrario,
- modificar el sistema de archivos para causar una denegación de servicio (DoS) u obtener privilegios de *root* en el sistema de archivos.

Se han asignado los siguientes identificadores identificadores: CVE-2020-3361, CVE-2020-3263, CVE-2020-3342, CVE-2020-3336, CVE-2020-3286, CVE-2020-3287, CVE-2020-3288, CVE-2020-3289, CVE-2020-3290, CVE-2020-3291, CVE-2020-3292, CVE-2020-3293, CVE-2020-3294, CVE-2020-3295, CVE-2020-3296, CVE-2020-3268, CVE-2020-3269, CVE-2020-3274, CVE-2020-3275, CVE-2020-3276, CVE-2020-3277, CVE-2020-3278 y CVE-2020-3279.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidades en el core de Drupal

Fecha de publicación: 18/06/2020

Importancia: Crítica

Recursos afectados:

Versiones anteriores a:

- 9.0.1;
- 8.9.1;
- 8.8.8;
- 7.72.

Descripción:

Se han publicado una nueva actualización de seguridad que soluciona tres vulnerabilidades en el núcleo de Drupal.

Solución:

Actualizar a las versiones 7.72, 8.8.8, 8.9.1 o 9.0.1.

Detalle:

- La API de formularios del core de Drupal no maneja adecuadamente ciertas entradas de formularios de peticiones de tipo cross-site, lo que puede conducir a otras vulnerabilidades. Se ha reservado el identificador CVE-2020-13663 para esta vulnerabilidad.
- Una vulnerabilidad de ejecución de código remoto bajo ciertas circunstancias, en Drupal 8 y 9, podría permitir a un atacante engañar a un administrador para que visitara un sitio malicioso, lo que podría resultar en la creación de un directorio cuidadosamente nombrado en el sistema de archivos. Con este directorio en su lugar, un atacante podría intentar forzar una vulnerabilidad de ejecución de código remoto. Los servidores de Windows son los más afectados. Se ha reservado el identificador CVE-2020-13664 para esta vulnerabilidad.
- Las solicitudes JSON:API PATCH pueden evitar la validación de ciertos campos. Por defecto, JSON:API funciona en modo de sólo lectura, lo que hace imposible explotar la vulnerabilidad. Sólo los sitios que tienen el *read_only* configurado como *FALSE* en *jsonapi.settings* son vulnerables. Se ha reservado el identificador CVE-2020-13665 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de Dell IMC

Fecha de publicación: 19/06/2020

Importancia: Alta

Recursos afectados:

- Dell EMC Isilon OneFS, versiones 8.2.2 y anteriores;
- Dell EMC PowerScale OneFS, versión 9.0.0;
- Dell EMC Unisphere para PowerMax, versiones anteriores a 9.1.0.17;
- Dell EMC Unisphere para PowerMax Virtual Appliance, versiones anteriores a 9.1.0.17;
- PowerMax OS Release 5978.

Descripción:

Dell ha informado de tres vulnerabilidades, dos de ellas descubiertas por Thorsten TÃ¤llmann, del Karlsruhe Institute of Technology, dos con severidad alta y una media, de tipo asignación incorrecta de permisos, validación de certificado incorrecta y omisión de autenticación.

Solución:

- Para Dell EMC Isilon OneFS y Dell EMC PowerScale OneFS, modificar los permisos en */ifs* como se muestra a continuación:

```
chmod 755 /ifs
chmod  a group admin allow generic_write,delete_child,std_write_dac /ifs
chmod  a user compadmin allow generic_write,delete_child,std_write_dac /ifs
```

- para Dell EMC Unisphere para PowerMax: actualizar a la versión 9.1.0.17 y posteriores;
- para Dell EMC Unisphere para PowerMax Virtual Appliance: actualizar a la versión 9.1.0.17 y posteriores;
- para PowerMax OS Release 5978.221.221 o 5978.479.479: el fabricante está trabajando en un *ePack* que lo solucione.

Detalle:

- Un atacante, con acceso a archivos de red o locales, podría aprovechar los permisos de archivos aplicados de manera insuficiente para obtener acceso no autorizado a dichos archivos, comprometiendo el sistema afectado. Se ha reservado el identificador CVE-2020-5371 para esta vulnerabilidad.
- Un atacante remoto, no autenticado, podría realizar un ataque de *man-in-the-middle* al proporcionar un certificado especialmente diseñado, e interceptar el tráfico del usuario para ver o modificar sus datos en tránsito. Se ha reservado el identificador CVE-2020-5367 para esta vulnerabilidad.

Para la vulnerabilidad de severidad media, se ha reservado el identificador CVE-2020-5345.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades de denegación de servicio en Squid

Fecha de publicación: 22/06/2020

Importancia: Alta

Recursos afectados:

Las siguientes versiones de Squid se ven afectadas por 2 vulnerabilidades:

- desde 3.1 hasta 3.5.28;
- desde 4.0 hasta 4.11;
- desde 5.0.1 hasta 5.0.2.

Descripción:

Los investigadores Jack Zar, de Bloomberg, y Christof Gerber y Mario Galli, de Open Systems AG, han descubierto dos vulnerabilidades, ambas con severidad alta, de tipo denegación de servicio (DoS).

Solución:

- Para la vulnerabilidad CVE-2020-14059, actualizar a la versión 5.0.3 o aplicar el parche para Squid 5;
- para la vulnerabilidad CVE-2020-14058, actualizar a las versiones 4.12 o 5.0.3, o aplicar los parches para Squid 4 o Squid 5.

Detalle:

- Debido a una sincronización incorrecta, Squid es vulnerable a un ataque de denegación de servicio (DoS) al procesar objetos en un caché SMP. Este problema podría permitir que un cliente remoto active una aserción de un *worker* de Squid. Se ha reservado el identificador CVE-2020-14059 para esta vulnerabilidad.
- Debido al uso de una función potencialmente peligrosa, Squid y el asistente de validación de certificados predeterminado son vulnerables a un ataque de denegación de servicio (DoS) al procesar certificados TLS. Se ha reservado el identificador CVE-2020-14058 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos VMware

Fecha de publicación: 25/06/2020

Importancia: Crítica

Recursos afectados:

- VMware ESXi, versiones 7.0, 6.7 y 6.5;
- VMware Workstation Pro / Player (Workstation), versiones 15.x;
- VMware Fusion Pro / Fusion (Fusion), versiones 11.x;
- VMware Cloud Foundation, versiones 4.x y 3.x.

Descripción:

VMware ha informado de múltiples vulnerabilidades en VMware ESXi, Workstation, y Fusion. En total se han notificado 10 vulnerabilidades siendo 1 crítica, 5 altas y 4 medias.

Solución:

Se recomienda instalar los últimos parches para los productos afectados en función de la versión estable utilizada:

- VMware ESXi: ESXi_7.0.0-1.20.16321839, o ESXi670-202004101-SG, o ESXi650-202005401-SG.
- VMware Workstation Pro / Player (Workstation): 15.5.5.
- VMware Fusion Pro / Fusion (Fusion): 11.5.5.
- VMware Cloud Foundation: 4.0.1 (pendiente de publicación), o 3.10 o 3.10.0.1 (pendiente de publicación).

Detalle:

La vulnerabilidad más crítica de las informadas por VMware permitiría a un atacante con acceso local a una máquina virtual con gráficos

3D habilitados ejecutar código en el hipervisor desde la propia máquina virtual por medio de una vulnerabilidad de tipo 'use-after-free' en la que se use memoria después de liberación en un dispositivo SVGA. Se ha asignado el identificador CVE-2020-3962 para esta vulnerabilidad.

Otros identificadores asignados para el resto de vulnerabilidades son CVE-2020-3963, CVE-2020-3964, CVE-2020-3965, CVE-2020-3966, CVE-2020-3967, CVE-2020-3968, CVE-2020-3969, CVE-2020-3970 y CVE-2020-3971.

Etiquetas: Actualización, Virtualización, VMware, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Dell EMC

Fecha de publicación: 25/06/2020

Importancia: Alta

Recursos afectados:

- Dell EMC Avamar Server, hardware appliance Gen4S, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP1;
- Dell EMC Avamar Server, hardware appliance Gen4T, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP3;
- Dell EMC Avamar Server, hardware appliance Gen4S/Gen4T, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP4;
- Dell EMC Avamar Server, hardware appliance Gen4S/Gen4T, versiones 19.2, en SUSE Linux Enterprise 12SP4;
- Dell EMC Avamar Server, hardware applianceGen4S/Gen4T, versiones 19.3, en SUSE Linux Enterprise 12SP5;
- Dell EMC Avamar Virtual Edition, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP3;
- Dell EMC Avamar Virtual Edition, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP4 (incluyendo Azure y AWS deployments desde la 7.5.1);
- Dell EMC Avamar Virtual Edition, versiones 19.2, en SUSE Linux Enterprise 12SP4 (incluyendo Azure y AWS deployments);
- Dell EMC Avamar Virtual Edition, versiones 19.3, en SUSE Linux Enterprise 12SP5 (incluyendo Azure y AWS deployments);
- Dell EMC Avamar NDMP Accelerator, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP1, SP3 y 12SP4;
- Dell EMC Avamar VMware Image Proxy, versiones 7.4 y posteriores, en SUSE Linux Enterprise 11SP1 o SUSE Linux Enterprise 11SP3;
- Dell EMC Avamar VMware Image Proxy, versiones 7.5.1 y posteriores, en SUSE Linux Enterprise 12SP1 o SUSE Linux Enterprise 12SP4;
- Dell EMC NetWoker Virtual Edition (NVE), versiones 18.x y posteriores, en SUSE Linux Enterprise 11SP3 o SP4;
- Dell EMC vCloud Directo Data Protection Extension, versiones 2.0.6 y posteriores, en SUSE Linux Enterprise 11SP3;
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.0, 2.1, 2.2, 2.3, 2.4 y 2.5;
- Dell Power Protect DataManager (PPDM), versiones anteriores a 19.4;
- Dell Power Protect X400 versiones anteriores a 3.2.

Descripción:

Se han publicado varias soluciones para vulnerabilidades que afectan a componentes de Dell EMC Avamar y NetWorker, así como otra vulnerabilidad en Dell Power Protect Data Manager que podría permitir a un atacante comprometer el sistema afectado.

Solución:

Aplicar las siguientes actualizaciones:

- SLES11 SP1/SP3/SP4, SLES12 SP4/SP5 Avamar: AvPlatformOsRollup_2020-R2-v6.avp;
- SLES11 SP3/SP4 NVE: NvePlatformOsRollup_2020-R2-v6.avp;
- Avamar Proxy Bundle 2020-R2-v6;
- Dell Power Protect Data Manager versión 19.4;
- Dell Power Protect X400 versión 3.2.

Detalle:

- Una vulnerabilidad de autorización inadecuada en Dell Power Protect Data Manager (PPDM) y Dell Power Protect X400 podría permitir a un atacante autenticado remotamente, la descarga de cualquier archivo de las máquinas virtuales Power Protect afectadas. Se ha reservado el identificador CVE-2020-5356 para esta vulnerabilidad.
- Varios componentes dentro de Dell EMC Avamar y NetWorker requieren una actualización de seguridad para abordar diversas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Denegación de servicio en HTTP/2 afecta a varias versiones de Apache Tomcat

Fecha de publicación: 26/06/2020

Importancia: Crítica

Recursos afectados:

Apache Tomcat, versiones:

- desde la 8.5.0 hasta la 8.5.55;
- desde la 9.0.0.M1 hasta la 9.0.35;
- desde la 10.0.0-M1 hasta la 10.0.0-M5.

Descripción:

Las versiones 8, 9 y 10 de Apache Tomcat están afectadas por una vulnerabilidad de denegación de servicio (DoS) que afecta al protocolo HTTP/2.

Solución:

Actualizar a las versiones:

- 8.5.56;
- 9.0.36;
- 10.0.0-M6.

Detalle:

Una secuencia, especialmente diseñada, de solicitudes HTTP/2 podría desencadenar un uso elevado de la CPU durante varios segundos. Si se realizara una cantidad suficiente de dichas solicitudes en conexiones HTTP/2 concurrentes, el servidor podría dejar de responder. Se ha reservado el identificador CVE-2020-11996 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Verificación incorrecta de la firma criptográfica en PAN-OS de Palo Alto Networks

Fecha de publicación: 30/06/2020

Importancia: Crítica

Recursos afectados:

PAN-OS, versiones:

- anteriores a 9.1.3;
- anteriores a 9.0.9;
- anteriores a 8.1.15;
- 8.0.*.

Descripción:

Los investigadores, Salman Khan, del Cyber Risk and Resilience Team, y Cameron Duck, del Identity Services Team, en Monash University, han descubierto una vulnerabilidad, de severidad crítica, de tipo verificación incorrecta de la firma criptográfica.

Solución:

La vulnerabilidad se soluciona en PAN-OS 8.1.15, PAN-OS 9.0.9, PAN-OS 9.1.3 y todas las versiones posteriores.

Detalle:

Cuando la autenticación SAML (*Security Assertion Markup Language*) está activada y la opción *Validate Identity Provider Certificate* desactivada, la verificación incorrecta de firmas en la autenticación SAML en PAN-OS podría permitir que un atacante, no autenticado, accediese a recursos protegidos de la red. El atacante debería tener acceso de red al servidor vulnerable para aprovechar esta vulnerabilidad. Este problema no podría ser aprovechado si SAML no se usa para la autenticación. Se ha asignado el identificador CVE-2020-2021 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad