Boletín de mayo de 2020

Avisos Técnicos

Múltiples vulnerabilidades en ShareFile storage zones Controller de Citrix

Fecha de publicación: 06/05/2020

Importancia: Crítica

Recursos afectados:

ShareFile storage zones Controller, versión 5.9.0 y anteriores.

Descripción:

El Danske Bank Red-Team, en colaboración con Citrix, ha detectado 3 vulnerabilidades de severidad crítica. Un atacante, no autenticado, podría divulgar información.

Solución:

Actualizar Storage Zones Controller a la versión:

- 5.10.0,
- 5.9.1,
- 5.8.1,
- 5.7.1,
- 5.6.1,
- 5.5.1.

Detalle:

Las vulnerabilidades detectadas podrían permitir a un atacante, no autenticado, comprometer los controladores de zonas de almacenamiento, pudiendo de este modo, acceder a la información que contenga el usuario en ShareFile. Se han reservado los identificadores CVE-2020-7473, CVE-2020-8982 y CVE-2020-8983, para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Salt de SaltStack

Fecha de publicación: 06/05/2020

Importancia: Crítica

Recursos afectados:

- Salt, versión 3000.1 y anteriores;
- Salt, versión 2019.2.3 y anteriores.

Descripción:

Investigadores de F-Secure han reportado a Salt dos vulnerabilidades de severidad crítica que afectan a su *Framework* Salt. Un atacante, remoto, podría evadir los controles de autenticación y ejecutar código arbitrario con privilegios de *root* en el sistema.

Solución:

- Actualizar Salt 3000.X a la versión 3000.2 o posterior.
- Actualizar Salt 2019.X a la versión 2019.2.4 o posterior.

Detalle:

- La clase ClearFuncs, del proceso Salt-master, no valida adecuadamente las llamadas a métodos. Un atacante remoto podría acceder algunos métodos evadiendo la autenticación. Se ha asignado el identificador CVE-2020-11651 para esta vulnerabilidad.
- La clase ClearFuncs, del proceso Salt-master, permite acceder a algunos métodos que sanean inapropiadamente las rutas. Un atacante remoto, autenticado, podría acceder a directorios. Se ha asignado el identificador CVE-2020-11652 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 07/05/2020

Importancia: Alta

Recursos afectados:

- Productos de Cisco si están ejecutando Cisco ASA (*Adaptive Security Appliance*), con autenticación Kerberos configurada para VPN, o acceso a dispositivos locales;
- productos de Cisco que ejecutan una versión vulnerable de Cisco ASA o Cisco FTD (*Firepower Threat Defense*), que están configurados para admitir el enrutamiento OSPF (*Open Shortest Path First*) con el procesamiento de bloques LLS (*Link-Local Signaling*) habilitado;
- productos de Cisco si están ejecutando una versión vulnerable de Cisco ASA o Cisco FTD y tienen una función habilitada para procesar mensajes SSL/TLS, pero no limitado a:
  - AnyConnect SSL VPN,
  - Clientless SSL VPN,
  - WebVPN,
  - servidor HTTP utilizado para la interfaz de administración;
- versiones vulnerables de Cisco ASA o Cisco FTD, cuando se configura con el protocolo IPv6;
- productos de Cisco si están ejecutando una versión vulnerable de Cisco ASA o Cisco FTD, y están configurados para inspeccionar el tráfico de MGCP (*Media Gateway Control Protocol*);
- Cisco FTD, versiones:
  - 6.3.0 y 6.4.0,
  - 6.2.3.12, 6.2.3.13, 6.2.3.14 y 6.2.3.15, si *VPN System Logging* está configurado;
- productos de Cisco si están ejecutando una versión vulnerable de Cisco FTD, y están configurados con una política de control de acceso para bloquear ciertos tipos de tráfico.

Descripción:

Diversos investigadores han descubierto 12 vulnerabilidades, todas de severidad alta, de tipo omisión de autenticación, mecanismos de protección de memoria inadecuados al procesar ciertos paquetes OSPF, gestión de recursos inadecuada para conexiones entrantes SSL/TLS, problema de seguimiento (*tracking*) del búfer en el análisis de URL, validación de longitud incorrecta de un campo en un paquete DNS IPv6, gestión de memoria ineficiente, falta de validación de entrada adecuada de la URL, error de gestión de memoria cuando se procesa el tráfico GRE (*Generic Routing Encapsulation*) sobre IPv6, liberación inadecuada de la memoria del sistema y error de comunicación entre funciones internas.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

Un atacante remoto, no autenticado, que aprovechase estas vulnerabilidades podría realizar alguna de las siguientes acciones:

- suplantar al KDC (*Key Distribution Center*) de Kerberos y omitir la autenticación,
- denegación de servicio (DoS),
- pérdida de memoria (*memory leak*),
- divulgación de información confidencial,
- reiniciar el dispositivo afectado,
- acceso a rutas no controlado (*path traversal*).

Se han asignado los siguientes identificadores: CVE-2020-3125, CVE-2020-3298, CVE-2020-3195, CVE-2020-3196, CVE-2020-3259, CVE-2020-3191, CVE-2020-3254, CVE-2020-3187, CVE-2020-3179, CVE-2020-3255, CVE-2020-3189 y CVE-2020-3283.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en BIG-IP de F5

Fecha de publicación: 12/05/2020

Importancia: Alta

Recursos afectados:

- BIG-IP (APM), versiones:
  - 15.0.0 - 15.1.0,
  - 14.1.0 - 14.1.2,
  - 13.1.0 - 13.1.3,
  - 12.1.0 - 12.1.5,
  - 11.6.1 - 11.6.5;
- BIG-IP APM Clients, versiones:
  - 7.1.5 - 7.1.9.

Descripción:

Juliette Chapalain, del Red Team/CERT Société Générale, ha descubierto dos vulnerabilidades, ambas de severidad alta, que afectan al producto BIG-IP Edge Client para Windows de F5, de tipo permisos insuficientes de archivos y carpetas, y uso la memoria previamente liberada.

Solución:

En la versión 13.1.0 de BIG-IP APM y posteriores, los componentes APM Clients pueden actualizarse independientemente del *software* BIG-IP, tal y como se indica en *K52547540: Updating BIG-IP Edge Client for the BIG-IP APM system* y *K13757: BIG-IP Edge Client version matrix*.

Detalle:

- La carpeta temporal de BIG-IP Edge Client Windows Installer Service tiene archivos y carpetas con permisos inadecuados, y permite la ejecución de archivos *.exe* y MSI firmados, lo que daría la posibilidad a un usuario, sin privilegios, de realizar una escalada de privilegios en el cliente de Windows. Se ha reservado el identificador CVE-2020-5896 para esta vulnerabilidad.
- Una vulnerabilidad, de tipo memoria previamente liberada, en BIG-IP Edge Client Windows ActiveX, permitiría que un atacante cause fallos en la memoria del navegador o ejecute código desde el navegador creando una página web maliciosa y cargándola en el navegador Internet Explorer, utilizado por los usuarios de BIG-IP Edge Client. Se ha reservado el identificador CVE-2020-5897 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Boletín de seguridad de Microsoft de mayo de 2020

Fecha de publicación: 13/05/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (basado en EdgeHTML);
- Microsoft Edge (basado en Chromium);
- ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Windows Defender;
- Visual Studio;
- Microsoft Dynamics;
- .NET Framework;
- .NET Core;
- Power BI.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de mayo, consta de 111 vulnerabilidades, 16 clasificadas como críticas y 95 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 restricciones de seguridad.

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Actualización de seguridad de SAP de mayo de 2020

Fecha de publicación: 13/05/2020

Importancia: Crítica

Recursos afectados:

- SAP Application Server ABAP, versiones 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710 y 740;
- SAP Business Client, versión 6.5;
- SAP Business Objects Business Intelligence Platform (Live Data Connect), versiones 1.0, 2.0 y 2.x;
- SAP Adaptive Server Enterprise (Backup Server), versión 16.0;
- SAP Business Objects Business Intelligence Platform (CrystalReports WebForm Viewer), versiones 4.1 y 4.2;
- SAP Adaptive Server Enterprise (Cockpit), versión 16.0;
- SAP Adaptive Server Enterprise, versión 16.0;
- SAP Application Server ABAP, versiones 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710 y 740;
- SAP Business Client, versión 6.5;
- SAP Business Objects Business Intelligence Platform (Live Data Connect), versiones 1.0, 2.0 y 2.x;
- SAP Adaptive Server Enterprise (Backup Server), versión 16.0;
- SAP Business Objects Business Intelligence Platform (CrystalReports WebForm Viewer), versiones 4.1 y 4.2;
- SAP Adaptive Server Enterprise (Cockpit), versión 16.0;
- SAP Adaptive Server Enterprise, versión 16.0;
- SAP Adaptive Server Enterprise (XP Server on Windows Platform), versiones 15.7 y 16.0;

- SAP Master Data Governance, versiones S4CORE 101; S4FND 102, 103 y 104; SAP_BS_FND 748;
- SAP Adaptive Server Enterprise (Web Services), versiones 15.7 y 16.0;
- SAP Business Client, versión 7.0;
- SAP Adaptive Server Enterprise, versión 16.0;
- SAP Business Objects Business Intelligence Platform, versión 4.2;
- SAP Adaptive Server Enterprise, versiones 15.7 y 16.0;
- SAP Enterprise Threat Detection, versiones 1.0 y 2.0;
- SAP Master Data Governance, versiones 748, 749, 750, 751, 752, 800, 801, 802, 803 y 804;
- SAP Business Objects Business Intelligence Platform (CMC y BI launchpad), versión 4.2;
- SAP Plant Connectivity, versiones 15.1, 15.2, 15.3 y 15.4;
- SAP NetWeaver AS ABAP (Web Dynpro ABAP), versiones SAP_UI 750, 752, 753 y 754; SAP_BASIS 700, 710, 730, 731 y 804;
- SAP Business Objects Business Intelligence Platform, versiones anteriores a la 4.1, 4.2 y 4.3;
- SAP Business Objects Business Intelligence Platform, versiones anteriores a la 4.1, 4.2 y 4.3;
- SAP Identity Management, versión 8.0.

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 18 notas de seguridad y 4 actualizaciones, siendo 6 de ellas de severidad crítica, 4 altas y 12 medias

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de inyección de código,
- 2 vulnerabilidades de *Cross-Site Scripting*,
- 2 vulnerabilidades de denegación de servicio,
- 3 vulnerabilidades de divulgación de información,
- 1 vulnerabilidad de falta de autenticación.
- 3 vulnerabilidades de falta de comprobación de autenticación,
- 3 vulnerabilidades de *SQL injection,*
- 7 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- La validación insuficiente de los datos de entrada en un módulo de función habilitado remotamente que genera código dinámicamente podría permitir a un atacante tomar el control completo de cualquier sistema ABAP de SAP NW que esté conectado a un sistema Solution Manager (SolMan). Se ha asignado el identificador CVE-2020-6262 para esta vulnerabilidad.
- La falta de comprobación de la autenticaciónSAP Business Objects Business Intelligence Platform (Live Data Connect), versiones 1.0, 2.0, 2.x, podría permitir a un atacante entrar en la consola central de gestión sin contraseña en caso de que el servidor de aplicaciones BIPRWS no estuviera protegido con algún certificado específico. Se ha asignado el identificador CVE-2020-6242 para esta vulnerabilidad.
- SAP Adaptive Server Enterprise (Backup Server), versión 16.0, no realiza las comprobaciones de validación necesarias para un usuario autentificado mientras ejecuta el comando DUMP o LOAD. Esto podría permitir a un atacante la ejecución de códigos arbitrarios o la inyección de códigos. Se ha asignado el identificador CVE-2020-6248 para esta vulnerabilidad.
- Bajo ciertas condiciones el SAP Adaptive Server Enterprise (Cockpit), podría permitir a un atacante con acceso a la red local, obtener información sensible y confidencial, pudiendo obtener credenciales de cuentas de usuario, manipular datos del sistema o influir en la disponibilidad del sistema. Se ha asignado el identificador CVE-2020-6252 para esta vulnerabilidad.

Los identificadores asignados para el resto de vulnerabilidades son: CVE-2020-6219, CVE-2020-6241, CVE-2020-6243, CVE-2020-6249, CVE-2020-6253, CVE-2020-6244, CVE-2020-6250, CVE-2020-6245, CVE-2020-6259, CVE-2020-6254, CVE-2020-6256, CVE-2020-6257, CVE-2020-6240, CVE-2019-0352, CVE-2019-0352 y CVE-2020-6258.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en productos de Palo Alto Networks

Fecha de publicación: 14/05/2020

Importancia: Crítica

Recursos afectados:

- PAN-OS 9.1, versiones anteriores a la 9.1.1;
- PAN-OS 9.0, versiones anteriores a la 9.0.7;
- PAN-OS 8.1, versiones anteriores a la 8.1.14;
- PAN-OS 8.0, todas las versiones;
- PAN-OS 7.1, todas las versiones.

Descripción:

Palo Alto Networks ha publicado 16 avisos de seguridad en su centro de seguridad de productos, 1 de severidad crítica y 15 de severidad alta.

Solución:

Actualizar a las siguientes versiones:

- PAN-OS 9.1, versión 9.1.1 o posterior;
- PAN-OS 9.0, versión 9.0.7 o posterior;
- PAN-OS 8.1, versión 8.1.14 o posterior.

PAN-OS 7.1 está en soporte extendido hasta el 30 de junio de 2020, y sólo se tiene en cuenta para las vulnerabilidades críticas de seguridad.

PAN-OS 8.0 ha llegado al final de su vida útil y no está cubierto por las pólizas de garantía de seguridad de productos del fabricante.

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades mencionadas, podría llegar a realizar las siguientes acciones en los productos afectados:

- escalada de privilegios,
- acceder a PAN-OS como administrador,
- comprometer la sesión del usuario activo,
- ejecutar código arbitrario con privilegios de *root*,
- ejecutar comandos del sistema operativo con privilegios de *root*,
- borrar archivos arbitrarios de sistema,
- comprometer la integridad del sistema,
- denegación de servicio (DoS),
- lectura arbitraria de archivos en el sistema,
- acceso a la cuenta de administrador y manipulación de dispositivos administrados por Panorama,
- ejecutar comandos *shell* arbitrarios con privilegios de *root*,
- cierre inesperado de los procesos del sistema,
- realizar acciones del administrador,
- obtener un acceso privilegiado a los cortafuegos gestionados.

Se han asignado los identificadores CVE-2020-2001, CVE-2020-2002, CVE-2020-2005, CVE-2020-2006, CVE-2020-2007, CVE-2020-2008, CVE-2020-2009, CVE-2020-2010, CVE-2020-2011, CVE-2020-2012, CVE-2020-2013, CVE-2020-2014, CVE-2020-2015, CVE-2020-2016, CVE-2020-2017 y CVE-2020-2018 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en IBM i2 Analysts Notebook

Fecha de publicación: 14/05/2020

Importancia: Alta

Recursos afectados:

IBM i2 Analysts Notebook e IBM i2 Analysts Notebook Premium, versión 9.2.1.

Descripción:

Los investigadores Honggang Ren y Kexu Wang, ambos pertenecientes a FortiGuard Labs de Fortinet, han notificado 15 vulnerabilidades a IBM, todas de severidad alta, de corrupción de memoria.

Solución:

Actualizar a las versiones IBM i2 Analysts Notebook 9.2.1.1 e IBM i2 Analysts Notebook Premium 9.2.1.1, respectivamente.

Detalle:

- IBM i2 Intelligent Analyis Platform podría permitir a un atacante local ejecutar código arbitrario en el sistema, causado por un fallo en la memoria. Al persuadir a un usuario para que abra un archivo especialmente diseñado, el atacante podría aprovechar esta vulnerabilidad para ejecutar código arbitrario en el sistema. Se han reservado los identificadores CVE-2020-4261, CVE-2020-4262, CVE-2020-4266, CVE-2020-4265, CVE-2020-4257, CVE-2020-4264, CVE-2020-4258 y CVE-2020-4263 para esta vulnerabilidad.
- IBM i2 Intelligent Analyis Platform podría permitir a un atacante remoto ejecutar código arbitrario en el sistema, causado por un fallo en la memoria. Al persuadir a un usuario para que abra un archivo especialmente diseñado, el atacante podría aprovechar esta vulnerabilidad para ejecutar código arbitrario en el sistema con los privilegios del usuario o hacer que la aplicación se bloquee. Se han reservado los identificadores CVE-2020-4468, CVE-2020-4343, CVE-2020-4422, CVE-2020-4285, CVE-2020-4288, CVE-2020-4467 y CVE-2020-4287 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de lectura fuera de límites en Exim

Fecha de publicación: 18/05/2020

Importancia: Alta

Recursos afectados:

Exim, versión 4.93 y anteriores.

Descripción:

Orange Tsai, del equipo de seguridad de DEVCORE, ha descubierto una vulnerabilidad, con severidad alta, de lectura fuera de límites en el método de autenticación SPA de Exim.

Solución:

Actualizar a la versión 4.94 de Exim.

Detalle:

Exim4 sufre una vulnerabilidad de lectura fuera de límites en el controlador de autenticación de SPA, que podría resultar en la omisión de autenticación SPA/NTLM en auths/spa.c y auths/auth-spa.c. Se ha asignado el identificador CVE-2020-12783 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de desbordamiento de enteros en PHP 7

Fecha de publicación: 18/05/2020

Importancia: Alta

Recursos afectados:

PHP7, versiones anteriores a la versión 7.4.6.

Descripción:

PHP ha detectado una vulnerabilidad de criticidad alta del tipo desbordamiento de enteros.

Solución:

Actualizar PHP 7 a la versión 7.4.6.

Detalle:

Un error en *php-src/main/rfc1867.c* asociado a la subida de archivos con nombre de archivos largos, podría generar un desbordamiento de enteros con un consecuente bloqueo. Un atacante remoto, que aprovechase esta vulnerabilidad, podría generar una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2019-11048 para esta vulnerabilidad.

Etiquetas: Actualización, PHP, Vulnerabilidad

Vulnerabilidad de denegación de servicio en IBM Spectrum Scale

Fecha de publicación: 19/05/2020

Importancia: Alta

Recursos afectados:

IBM Spectrum Scale, versiones:

- desde 5.0.0.0, hasta 5.0.4.3;
- desde 4.2.0.0, hasta 4.2.3.21.

Descripción:

Se ha identificado una vulnerabilidad, de severidad alta, en todos los niveles de IBM Spectrum Scale, que podría permitir a un atacante local causar una denegación de servicio.

Solución:

- IBM Spectrum Scale desde 5.0.0.0, hasta 5.0.4.3, actualizar a 5.0.4.4;
- IBM Spectrum Scale desde 4.2.0.0, hasta 4.2.3.21, actualizar a 4.2.3.22.

Detalle:

El componente del sistema de archivos de IBM Spectrum Scale está afectado por una vulnerabilidad en su módulo del núcleo, que podría permitir que un atacante genere una condición de denegación de servicio en el sistema afectado. Para aprovechar esta vulnerabilidad, un atacante local podría invocar un subconjunto de *ioctls* (*input/output controls*) en el dispositivo Spectrum Scale con argumentos no válidos, provocando el bloqueo del núcleo. Se ha reservado el identificador CVE-2020-4411 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 19/05/2020

Importancia: Alta

Recursos afectados:

- Desde la versión 3.8, hasta la 3.8.2;
- desde la versión 3.7, hasta la 3.7.5;
- desde la versión 3.6, hasta la 3.6.9;
- desde la versión 3.5, hasta la 3.5.11;
- versiones anteriores sin soporte.

Descripción:

Los investigadores, Paul Holden y Abdullah Hussam, han reportado dos vulnerabilidades de criticidad alta del tipo ejecución remota de código y Cross-Site Scripting (XSS) almacenado.

Solución:

Moodle ha publicado diversas actualizaciones en función de la versión afectada:

- 3.8.3,
- 3.7.6,
- 3.6.10,
- 3.5.12.

Detalle:

- La versión 2.7.2 de MathJax, y anteriores, contienen una vulnerabilidad del tipo XSS almacenado. Se ha asignado el CVE-2018-1999024 para esta vulnerabilidad.
- Es posible generar un paquete SCORM, que cuando es añadido a un curso, puede conllevar a una ejecución remota de código. Se ha reservado el identificador CVE-2020-10738 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidades en BIND 9 de ISC

Fecha de publicación: 20/05/2020

Importancia: Alta

Recursos afectados:

Versiones de BIND afectadas:

- desde la 9.0.0, hasta la 9.11.18;
- desde la 9.12.0, hasta la 9.12.4-P2;
- desde la 9.14.0, hasta la 9.14.11;
- desde la 9.16.0, hasta la 9.16.2;
- desde la 9.17.0, hasta la 9.17.1 de la rama de desarrollo experimental 9.17;
- todas las versiones obsoletas de las ramas de desarrollo 9.13 y 9.15;
- todas las versiones de BIND Supported Preview Edition, desde la versión 9.9.3-S1, hasta la 9.11.18-S1.

Descripción:

Varios investigadores han reportado a ISC dos vulnerabilidades de criticidad alta.

Solución:

Actualizar a las siguientes versiones de BIND:

- BIND 9.11.19,
- BIND 9.14.12,
- BIND 9.16.3,
- BIND Supported Preview Edition, actualizar a la versión BIND 9.11.19-S1.

Detalle:

- Debido a una limitación insuficientemente restrictiva en el número de búsquedas mientras se procesa una respuesta, un atacante remoto podría impactar sobre el rendimiento del sistema, o emplear el servidor como reflector en un ataque de amplificación. Se ha asignado el identificador CVE-2020-8616 para esta vulnerabilidad.
- Un error en el código que comprueba la validez de los mensajes que contengan registros TSIG podría permitir a un atacante remoto, generar una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-8617 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, DNS, Vulnerabilidad

---

Vulnerabilidad de inyección de código en Cloud Director de VMware

Fecha de publicación: 20/05/2020

Importancia: Alta

Recursos afectados:

vCloudDirector, versiones:

- 10.0.x, para Linux y PhotonOS appliance;
- 9.7.x, para Linux y PhotonOS appliance;
- 9.5.x, para Linux y PhotonOS appliance;
- 9.1.x, para Linux.

Descripción:

Dos investigadores de Citadelo han reportado a VMware una vulnerabilidad de criticidad alta del tipo inyección de código.

Solución:

Actualizar las versiones afectadas de vCloud Director a las versiones:

- 10.0.0.2,
- 9.7.0.5,
- 9.5.0.6,
- 9.1.0.4.

Detalle:

VMware Cloud Director no maneja adecuadamente las entradas, por lo que un atacante remoto podría realizar una inyección de código. Se ha reservado el identificador CVE-2020-3956 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos HPE

Fecha de publicación: 20/05/2020

Importancia: Crítica

Recursos afectados:

- HPE Superdome Flex Server, versión anterior a la 3.25.46;
- Nimble Storage Hybrid Flash Arrays, Nimble Storage All Flash Arrays y Nimble Storage Secondary Flash Arrays, versiones 3.9.2.0, 4.5.5.0, 5.0.8.0, 5.1.4.0 y anteriores.

Descripción:

HPE ha publicado 3 vulnerabilidades, 2 críticas y una alta, en Superdome Flex Server y HPE NimbleOS que podrían permitir a un atacante la escalada de privilegios o acceder y modificar información sensible y de sistema.

Solución:

- HPE Superdome Flex Server, actualizar a la versión 3.25.46 o posterior;
- HPE NimbleOS, actualizar a las versiones 3.9.3.0, 4.5.6.0, 5.0.9.0, 5.1.4.100 o posteriores.

Detalle:

- Un fallo de validación en un componente de HPE Superdome Flex Server podría permitir a un atacante local la escalada de privilegios. Se ha asignado el identificador CVE-2020-7137 para esta vulnerabilidad.
- Vulnerabilidades de ejecución remota de código en los sistemas HPE Nimble Storage podrían permitir a un atacante la escalada de privilegios en el vector. Se ha asignado el identificador CVE-2020-7138 para esta vulnerabilidad.
- Vulnerabilidades de acceso remoto en los sistemas HPE Nimble Storage podrían permitir a un atacante acceder y modificar información sensible o de sistema. Se ha asignado el identificador CVE-2020-7139 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en JasperReports de TIBCO

Fecha de publicación: 20/05/2020

Importancia: Crítica

Recursos afectados:

- TIBCO JasperReports Server, versiones:
  - 7.5.0;
  - 7.2.0;
  - 7.1.1 y anteriores;
- TIBCO JasperReports Server para AWS Marketplace, versión 7.5.0 y anteriores;
- TIBCO JasperReports Server para ActiveMatrix BPM, versión 7.1.1 y anteriores;
- TIBCO JasperReports Library, versiones:
  - 7.5.0;
  - 7.3.0;
  - 7.2.1;
  - 7.2.0;
  - 7.1.1 y anteriores;
- TIBCO JasperReports Library para ActiveMatrix BPM, versión 7.1.1 y anteriores;
- los componentes *administrative UI* y *report generator*.

Descripción:

Se han identificado dos vulnerabilidades, una de severidad crítica y otra alta, de tipo escalada de privilegios e inyección HTML.

Solución:

- TIBCO JasperReports Server:
  - versión 7.1.1 y anteriores, actualizar a 7.1.3 o posteriores;
  - versión 7.2.0 y anteriores, actualizar a 7.2.1 o posteriores;
  - versión 7.5.0 y anteriores, actualizar a 7.5.1 o posteriores;
- TIBCO JasperReports Server para AWS Marketplace, versión 7.5.0 y anteriores, actualizar a 7.5.1 o posteriores;
- TIBCO JasperReports Server para ActiveMatrix BPM, versión 7.1.1 y anteriores, actualizar a 7.1.3 o posteriores;
- TIBCO JasperReports Library:
  - versión 7.1.1 y anteriores, actualizar a 7.1.3 o posteriores;
  - versiones 7.2.0 y 7.2.1, actualizar a 7.2.2 o posteriores;
  - versión 7.3.0, actualizar a 7.3.1 o posteriores;
  - versión 7.5.0, actualizar a 7.5.1 o posteriores;
- TIBCO JasperReports Library para ActiveMatrix BPM, versión 7.1.1 y anteriores, actualizar a 7.1.3 o posteriores.

Detalle:

- Un atacante remoto, sin autenticar, podría obtener permisos de *superuser* en JasperReports Server y ejecutar código arbitrario en

el sistema afectado. Se ha reservado el identificador CVE-2020-9409 para esta vulnerabilidad.
- Un atacante podría realizar una inyección HTML (también conocido como XSS persistente) para obtener el control total de una interfaz web que contiene la salida del componente generador de informes, pudiendo obtener así el nivel de privilegios del propietario con más privilegios que visualice un informe especialmente diseñado. Se ha reservado el identificador CVE-2020-9410 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 21/05/2020

Importancia: Crítica

Recursos afectados:

- Cisco Unified Contact Center Express (CCX), versión 12.0 y anteriores;
- Cisco Prime Network Registrar, versiones 8.3, 9.0, 9.1, 10.0 y 10.1.

Descripción:

Brenden Meeder, de Booz Allen Hamilton, y Cisco Technical Assistance Center (TAC) han reportado 2 vulnerabilidades, de severidad crítica y alta, de tipo validación de entrada incorrecta en ambos casos.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas, detalladas en la sección *Fixed Releases* de cada aviso, pueden descargarse desde el panel de descarga de Software Cisco.

Detalle:

Un atacante remoto, no autenticado, que aprovechase estas vulnerabilidades podría realizar alguna de las siguientes acciones:

- ejecución remota de código,
- denegación de servicio (DoS).

Se han reservado los siguientes identificadores: CVE-2020-3280 y CVE-2020-3272.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de denegación de servicio en Windows DNS Server de Microsoft

Fecha de publicación: 21/05/2020

Importancia: Alta

Recursos afectados:

Todas las versiones de Windows DNS Server.

Descripción:

Los investigadores, Yehuda Afek y Lior Shafir, de la Universidad de Tel-Aviv, y Anat Bremler-Barr, del IDC Herzliya, han alertado a Microsoft de una vulnerabilidad que afecta a los servidores DNS de Windows. Un atacante podría aprovechar esta vulnerabilidad para causar una condición de denegación de servicio.

Solución:

Como medida de mitigación para el problema de amplificación de DNS, en caso de que la víctima esté utilizando el servidor DNS de Microsoft, se recomienda habilitar la funcionalidad *Response Rate Limit* (RRL).

Detalle:

Un atacante podría aprovechar esta vulnerabilidad, relacionada con la amplificación de paquetes que afecta a los servidores DNS de Windows, para provocar una condición de denegación de servicio distribuido (DDoS), consiguiendo que el servicio del servidor DNS dejara de responder.

Etiquetas: DNS, Microsoft, Vulnerabilidad, Windows

Vulnerabilidad de ejecución remota de código en Apache Tomcat

Fecha de publicación: 21/05/2020

Importancia: Alta

Recursos afectados:

Apache Tomcat, versiones:

- desde la 7.0.0, hasta la 7.0.103;
- desde la 8.5.0, hasta la 8.5.54;
- desde la 9.0.0.M1, hasta la 9.0.34;
- desde la 10.0.0-M1, hasta la 10.0.0-M4.

Descripción:

El investigador Jarvis Threedr3am, de pdd security research, ha reportado al equipo de seguridad de Apache Tomcat una vulnerabilidad de criticidad alta del tipo ejecución remota de código.

Solución:

Actualizar Apache Tomcat a las siguientes versiones:

- 7.0.104,
- 8.5.55,
- 9.0.35,
- 10.0.0-M5.

Detalle:

Un atacante remoto, que envíe una respuesta específicamente creada, podría realizar una ejecución remota de código mediante la deserialización del archivo bajo su control. Se ha asignado el identificador CVE-2020-9484 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Vulnerabilidades en el core de Drupal

Fecha de publicación: 21/05/2020

Importancia: Media

Recursos afectados:

Versiones anteriores a:

- 8.8.6;
- 8.7.14;
- 7.70.

Descripción:

Se han publicado dos vulnerabilidades de seguridad en jQuery que afectan a algunas versiones de Drupal. Así como una vulnerabilidad de redireccionamiento abierto en Drupal 7.

Solución:

Actualizar a las versiones 8.8.6, 8.7.14 o 7.70.

Detalle:

- Dos vulnerabilidades de XXS en jQuery podrían permitir a un atacante ejecutar código no confiable al pasar un HTML de fuentes no confiables, incluso después de sanearlo, a uno de los métodos de manipulación DOM de jQuery (es decir, *.html()*, *.append()*, y otros). Se han asignado los identificadores CVE-2020-11022 y CVE-2020-11023 para estas vulnerabilidades.
- Una vulnerabilidad de redireccionamiento abierto en Drupal 7, debida a una validación insuficiente del parámetro de consulta de destino en la función *drupal_goto()*, podría permitir a un atacante engañar a los usuarios para que visiten un enlace especialmente diseñado que los redirija a una URL externa arbitraria.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de inyección SQL en GESIO

Fecha de publicación: 26/05/2020

Importancia: Crítica

Recursos afectados:

GESIO ERP, versiones anteriores a la 11.2.

Descripción:

INCIBE ha coordinado la publicación de una vulnerabilidad en el software GESIO ERP, con el código interno INCIBE-2020-225, que ha sido descubierto por Francisco Palma, Luis Vázquez y Diego León.

Se ha asignado el código CVE-2020-8967 para esta vulnerabilidad. Se ha calculado una puntuación base de 10 según CVSS v3; siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H.

Solución:

Actualizar a la versión 11.2.

Detalle:

GESIO ERP es vulnerable a una INYECCIÓN SQL en el parámetro URL "idsite", incluido en el archivo cms_plantilla_sites.php.

La explotación de esta vulnerabilidad podría permitir a un atacante remoto ejecutar, al menos, tres tipos de acciones:

- ataque basado en error,
- ataque basado en tiempo,
- ataque por unión.

Debido a esta vulnerabilidad, un atacante podría ser capaz de recuperar toda la información de la base de datos.

GESIO ha desplegado las siguientes acciones para solucionar este problema:

- Mejoras en los procedimientos internos.
- Implementación de nuevos controles de programación anti-inyección en el frontend que estarán disponibles desde la versión 11.2.
- Mejoras adicionales en las funciones del backend, que también estarán disponibles desde la versión 11.2.

CWE-89: Neutralización incorrecta de elementos especiales usados en un comando SQL (Inyección SQL).

Línea temporal:

02/04/2019 ? Descubrimiento de los investigadores.

08/04/2020 ? Investigadores contactan con INCIBE.

21/04/2020 ? El equipo de seguridad de GESIO confirma a INCIBE la vulnerabilidad, indicando que la versión de corrección y el parche del software de lanzamiento han sido publicados en la v11.2 (Parche de seguridad).

01/06/2020 ? El aviso es publicado por INCIBE.

Si tiene más información sobre este aviso, póngase en contacto con INCIBE, como se indica en el reporte de vulnerabilidades al CNA.

Etiquetas: 0day, Actualización, CNA, Vulnerabilidad

Múltiples vulnerabilidades en productos de VMware

Fecha de publicación: 29/05/2020

Importancia: Alta

Recursos afectados:

- VMware ESXi, versiones 6.7 y 6.5;
- VMware Workstation Pro / Player (Workstation), versión 15.X;
- VMware Fusion Pro / Fusion (Fusion), versión 11.X;
- VMware Remote Console para Mac (VMRC para Mac), versión 11.X, y anteriores;
- VMware Horizon Client para Mac, versión 5.X, y anteriores.

Descripción:

Varios investigadores en ciberseguridad han notificado a VMware tres vulnerabilidades, una de criticidad alta, una media y otra baja, del tipo escalada de privilegios, control de acceso inapropiado y cierre inesperado del sistema.

Solución:

VWware ha publicado diversas actualizaciones en función del producto y versiones afectadas. Para obtener la actualización específica consulte el apartado *Referencias*.

Detalle:

- La vulnerabilidad de criticidad alta afecta a los productos de VMware Fusion, VMRC para Mac y Horizont Client para Mac. Estos productos contienen una vulnerabilidad de escalada local de privilegios, debido a un fallo en el *Time-of-check Time-of-use* (TOCTOU) del *service opener*. Un atacante, con privilegios normales, podría realizar una escalada de privilegios y obtener privilegios de *root* en el sistema. Se ha reservado el identificador CVE-2020-3957 para esta vulnerabilidad.
- A las vulnerabilidades de criticidad media y baja se les han reservado los identificadores CVE-2020-3958 y CVE-2020-3959, respectivamente.

Etiquetas: Actualización, VMware, Vulnerabilidad

Vulnerabilidades en Security Identity Governance and Intelligence (IGI) de IBM

Fecha de publicación: 29/05/2020

Importancia: Alta

Recursos afectados:

IBM Security Identity Governance and Intelligence, versión 5.2.6.

Descripción:

IBM ha publicado una vulnerabilidad de contraseñas embebidas y otra de inyección de XML External Entity Injection (XEE) en su producto Security Identity Governance and Intelligence (IGI).

Solución:

Actualizar a la versión 5.2.6.0-ISS-SIGI-FP0001.

Detalle:

- IBM ha eliminado las contraseñas embebidas presentes en la versión de IBM Security Directory Integrator utilizada por IBM Security Identity Governance and Intelligence (IGI).
- Virtual Appliance es vulnerable a un ataque de Inyección de Entidad Externa XML (XXE) que podría permitir a un atacante exponer información sensible o consumir recursos de memoria. Se ha asignado el identificador CVE-2020-4246 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad