Boletín de diciembre de 2019

Avisos Técnicos

Múltiples vulnerabilidades en Liferay

Fecha de publicación: 04/12/2019

Importancia: Crítica

Recursos afectados:

Liferay Portal, versión 7.2.0 y anteriores.

Descripción:

Se han detectado 6 vulnerabilidades, una con severidad crítica y cinco con severidades altas. Un atacante remoto podría obtener credenciales de usuario, ejecución o inyección de código, generar una condición de denegación de servicio (DoS) o realizar acciones sin autorización sobre los recursos del sistema.

Solución:

Actualizar la versión Liferay Portal 7.2.1 o posterior, cuando esté disponible.

Detalle:

- La vulnerabilidad de severidad crítica podría permitir a un atacante remoto ejecutar código a través de JSON web services (JSONWS).
- Las vulnerabilidades catalogadas como altas son debidas a:
  - un fallo en el widget «*Sing In*» podría revelar las credenciales del usuario en el HTLM.
  - una vulnerabilidad de redirección abierta en los Ajustes de la Cuenta (*Account Settings*).
  - la API JSONWS */user/send-password-by-** podría ser utilizada para generar una condición de denegación de servicio en el servidor de correo.
  - múltiples errores en los permisos podrían permitir a usuarios realizar acciones no autorizadas sobre los recursos del sistema.
  - múltiples vulnerabilidades del tipo *Cross-site-scripting* (XSS) podrían permitir la inyección de código.

Etiquetas: CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 05/12/2019

Importancia: Crítica

Recursos afectados:

- D3600, versiones anteriores a la versión 1.0.0.76;
- D6000, versiones anteriores a la versión 1.0.0.76;
- D6200, versiones anteriores a la versión 1.1.00.36;
- D7000, versiones anteriores a la versión 1.0.1.74;
- D7000v2, versiones anteriores a la versión 1.0.0.53;
- DM200, versiones anteriores a la versión 1.0.0.58;
- EX3700, versiones anteriores a la versión 1.0.0.70;
- EX3800, versiones anteriores a la versión 1.0.0.70;
- EX6000, versiones anteriores a la versión 1.0.0.30;
- EX6100, versiones anteriores a la versión 1.0.2.24;
- EX6120, versiones anteriores a la versión 1.0.0.40;
- EX6130, versiones anteriores a la versión 1.0.0.22;
- EX6150v1, versiones anteriores a la versión 1.0.0.42;
- EX6200, versiones anteriores a la versión 1.0.3.88;

- EX7000, versiones anteriores a la versión 1.0.0.66;
- JR6150, versiones anteriores a la versión 1.0.1.24;
- MR1100, versiones anteriores a la versión 12.06.08.00;
- PR2000, versiones anteriores a la versión 1.0.0.28;
- R6020, versiones anteriores a la versión 1.0.0.42;
- R6050, versiones anteriores a la versión 1.0.1.24;
- R6080, versiones anteriores a la versión 1.0.0.42;
- R6120, versiones anteriores a la versión 1.0.0.48;
- R6220, versiones anteriores a la versión 1.1.0.86;
- R6230, versiones anteriores a la versión 1.1.0.86;
- R6260, versiones anteriores a la versión 1.1.0.64;
- R6700, versiones anteriores a la versión 1.0.2.6;
- R6700v2, versiones anteriores a la versión 1.2.0.62;
- R6800, versiones anteriores a la versión 1.2.0.62;
- R6900, versiones anteriores a la versión 1.0.2.4;
- R6900P, versiones anteriores a la versión 1.3.1.64;
- R6900v2, versiones anteriores a la versión 1.2.0.62;
- R7000, versiones anteriores a la versión 1.0.9.60;
- R7000P, versiones anteriores a la versión 1.3.1.64;
- R7800, versiones anteriores a la versión 1.0.2.60;
- R7900, versiones anteriores a la versión 1.0.3.8;
- R7900P, versiones anteriores a la versión 1.4.1.30;
- R8000, versiones anteriores a la versión 1.0.4.46;
- R8000P, versiones anteriores a la versión 1.4.1.30;
- R8300, versiones anteriores a la versión 1.0.2.128;
- R8500, versiones anteriores a la versión 1.0.2.128;
- R8900, versiones anteriores a la versión 1.0.4.12;
- R9000, versiones anteriores a la versión 1.0.4.12;
- RAX40, versiones anteriores a la versión 1.0.3.64;
- WAC505, versiones anteriores a la versión 8.2.1.16;
- WAC510, versiones anteriores a la versión 8.2.1.16;
- WN2500RPv2, versiones anteriores a la versión 1.0.1.54;
- WNR2000v5, versiones anteriores a la versión 1.0.0.72;
- WNR2020, versiones anteriores a la versión 1.1.0.62;
- WNR614, versiones anteriores a la versión 1.1.0.54;
- XR500, versiones anteriores a la versión 2.3.2.56;
- XR700, versiones anteriores a la versión 1.0.1.20;

Descripción:

Netgear ha publicado 21 vulnerabilidades, 1 de severidad crítica y 20 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:

- La vulnerabilidad de severidad crítica podría permitir a un atacante evadir la autenticación del dispositivo afectado.
- Las vulnerabilidades de severidad alta podrían permitir a un atacante realizar las siguientes acciones:
  - CSRF (*Cross Site Request Forgery*),
  - evasión de autenticación,
  - desbordamiento del búfer antes de la autenticación,
  - desbordamiento de la pila antes de la autenticación,
  - acceso no autorizado,
  - inyección de comandos después de la autenticación,
  - desbordamiento del búfer después de la autenticación,
  - generar una condición de denegación de servicio,
  - divulgación de información sensible,
  - divulgación de las credenciales de administrador.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Verificación inadecuada de autenticación en Palo Alto PAN-OS

Fecha de publicación: 05/12/2019

Importancia: Alta

Recursos afectados:

- PAN-OS 7.1, versiones anteriores a la 7.1.25;
- PAN-OS 8.0, versiones anteriores a la 8.0.20;
- PAN-OS 8.1, versiones anteriores a la 8.1.11;
- PAN-OS 9.0, versiones anteriores a la 9.0.5.

Descripción:

Palo Alto ha publicado una vulnerabilidad en PAN-OS que podría permitir a un atacante escalar privilegios

Solución:

Actualizar a las versiones 7.1.25, 8.0.20, 8.1.11, 9.0.5 o posteriores.

Detalle:

Una comprobación de autenticación inadecuada en PAN-OS de Palo Alto Networks podría permitir a un atacante, con un rol personalizado de permisos reducidos, escalar privilegios y convertirse en superusuario. Este problema sólo afecta a los dispositivos configurados con el rol mencionado anteriormente. Se ha reservado el identificador CVE-2019-17437 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Cuenta IPMI por defecto en DataPower Gateway de IBM

Fecha de publicación: 10/12/2019

Importancia: Alta

Recursos afectados:

IBM DataPower Gateway, versiones 2018.4.1.0-2018.4.1.5 y 7.6.0.0-7.6.0.14.

Descripción:

Cuando se activa la opción IPMI sobre LAN también se habilita, automáticamente, la cuenta de administrador por defecto.

Solución:

Actualizar a:

- IBM DataPower Gateway 2018.4.1.6 (APAR IT29004);
- IBM DataPower Gateway 7.6.0.15 (APAR IT29004);

Detalle:

IBM DataPower Appliance e IBM MQ Appliance, tienen una cuenta de administrador predeterminada que se activa si el canal LAN IPMI está activado. Un atacante remoto podría utilizar esta cuenta para obtener acceso no autorizado al BMC. Se ha asignado el identificador CVE-2019-4621 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidad de ejecución remota en productos VMware

Fecha de publicación: 10/12/2019

Importancia: Crítica

Recursos afectados:

- VMware ESXi, versiones:
  - 6.7,
  - 6.5,
  - 6.0.
- VMware Horizon DaaS, rama de versiones 8.x.

Descripción:

El equipo de 360Vulcan, de la competición Tianfu Cup Pwn Contest 2019, ha detectado una vulnerabilidad de severidad crítica que afecta a múltiples productos de VMware. Un atacante remoto podría ejecutar código en el sistema.

Solución:

- VMware ha publicado diversos parches de seguridad para VMware ESXi según la versión afectada:
  - 6.7, aplicar el parche ESXi670-201912001.
  - 6.5, aplicar el parche ESXi650-201912001.
  - 6.0, aplicar el parche ESXi600-201912001.
- Para Horizon DaaS, se han publicado una serie de Hotfix para mitigar la vulnerabilidad hasta que se publique una actualización que solucione la misma.

Detalle:

Una vulnerabilidad de sobreescritura dinámica de memoria (heap) en el servicio OpenSLP podría permitir a un atacante remoto, con acceso al puerto 427, realizar una ejecución de código en el sistema. Se ha asignado el identificador CVE-2019-5544 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Múltiples vulnerabilidades en productos de Dell EMC

Fecha de publicación: 10/12/2019

Importancia: Crítica

Recursos afectados:

- Dell EMC Data Protection Advisor, versiones:

    - 6.3;
    - 6.4;
    - 6.5;
    - 18.1;
    - 18.2 anterior al *patch* 83;
    - 19.1 anterior al *patch* 71.
- Integrated Data Protection Appliance, versiones:
    - 2.0;
    - 2.1;
    - 2.2;
    - 2.3;
    - 2.4.

Descripción:

El API REST de la aplicación DPA, dentro del software Dell EMC Data Protection Advisor, contiene correcciones para múltiples vulnerabilidades que pueden ser explotadas por atacantes para comprometer el sistema afectado.

Solución:

Los usuarios registrados en el portal de soporte de Dell EMC pueden descargar las versiones listadas a continuación para corregir estas vulnerabilidades:

- Dell EMC Data Protection Advisor, versiones:
    - 19.2;
    - 19.1 con *patch* 71 o posterior;
    - 18.2 con *patch* 83 o posterior.
    - para las versiones 6.3, 6.4, 6.5, o 18.1: actualizar al *patch* 83 o posterior de la versión 18.2, o al *patch* 71 o posterior de la versión 19.1.
- Integrated Data Protection Appliance:
    - para las versiones 2.0, 2.1 o 2.2: actualizar a la versión 2.3 y aplicar el *patch* 83 o posterior de la versión 18.2 de Dell EMC Data Protection Advisor;
    - para las versiones 2.3 o 2.4: aplicar el *patch* 83 o posterior de la versión 18.2 de Dell EMC Data Protection Advisor.

Detalle:

- Existe una vulnerabilidad de falta de autenticación en el servidor en el API REST. Un usuario malicioso, remoto y con privilegios administrativos, puede explotar esta vulnerabilidad para alterar la lista permitida de comandos del sistema operativo de la aplicación, lo que podría llevar a la ejecución arbitraria de comandos del sistema operativo, ya que el usuario normal ejecuta el servicio DPA en el sistema afectado. Se ha reservado el identificador CVE-2019-18581 para esta vulnerabilidad.
- Se ha identificado una vulnerabilidad de inyección de plantilla en el lado del servidor en el API REST. Un usuario malicioso, remoto y con privilegios administrativos, puede explotar esta vulnerabilidad para inyectar *scripts* de generación de informes maliciosos en el servidor. Esto puede llevar a la ejecución de comandos del sistema operativo, ya que el usuario normal ejecuta el servicio DPA en el producto afectado. Se ha reservado el identificador CVE-2019-18582 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades en múltiples productos de Intel

Fecha de publicación: 11/12/2019

Importancia: Alta

Recursos afectados:

- Herramientas Administrativas de Linux para Intel(R) Network Adapters, versiones anteriores a la 24.3.
- Las generaciones de procesadores Intel Core 6ª, 7ª, 8ª, 9ª y 10ª.
- Procesadores Intel Xeon de las familias:
    - E3 v5 y v6,
    - E-2100,
    - E-2200.
- Intel NUC 8:
    - Mainstream Game Kit,
    - Mainstream Game Mini Computer,
    - Home - NUC8i3CYSM.
- Intel NUC Kit:
    - NUC8i7BEK,
    - NUC8i7HNK,
    - NUC7i7DNKE,
    - NUC7i5DNKE,
    - NUC7i3DNHE,
    - NUC6i7KYK,
    - NUC6i5SYH,
    - NUC7CJYH,
    - NUC6CAYS.
- Intel Compute Card:
    - CD1P64GK,
    - CD1M3128MK,
    - CD1IV128MK.
- Intel Compute Stick:
    - STK2mv64CC,
    - STK2m3W64CC.
- Intel NUC Board:
    - DE3815TYBE,
    - D34010WYB.

Descripción:

Intel ha descubierto siete vulnerabilidades de criticidad alta en múltiples productos. Un atacante local podría realizar una escalada de privilegios o revelar información sensible.

Solución:

- Para Herramientas Administrativas de Linux para Intel(R) Network Adapters, actualizar a la versión 24.3 o posterior.
- Para las familias de procesadores afectados, Intel recomienda actualizar la BIOS a la última versión disponible.
- Para las familias de Intel NUC, actualizar a la última versión del *firmware* disponible. Para más información, puede acceder a la sección de «Referencias».

Detalle:

- Una protección insuficiente de la memoria en las Herramientas Administrativas de Linux para Intel(R) Network Adapters podría permitir a un atacante local, autenticado, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-0159 para esta vulnerabilidad.
- Debido a unas comprobaciones inadecuadas de los ajustes de voltaje en varios procesadores Intel, podrían permitir a un atacante local, autenticado, realizar una escalada de privilegios o revelar información. Se ha reservado el identificador CVE-2019-11157 para esta vulnerabilidad.
- Vulnerabilidades de Intel NUC:
  - Restricciones del búfer indebidas podrían permitir a un atacante local, no autenticado, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-14608 para esta vulnerabilidad.
  - Un control de acceso indebido podría permitir a un atacante local, no autenticado, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-14610 para esta vulnerabilidad.
  - Una validación de parámetros de entrada indebida podría permitir a un atacante local, con privilegios, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-14609 para esta vulnerabilidad.
  - Un desbordamiento de enteros podría permitir a un atacante local, con privilegios, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-14611 para esta vulnerabilidad.
  - Una escritura fuera de límites podría permitir a un atacante local, con privilegios, realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-14612 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de diciembre de 2019

Fecha de publicación: 11/12/2019

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5;
- SAP Adaptive Server Enterprise, versiones 15.7 y 16.0;
- SAP BusinessObjects Business Intelligence Platform (Fiori BI Launchpad), versión 4.2;
- SAP ERP HCM (SAP_HRCES), versión 3;
- SAP Enable Now, versión 1911;
- SAP Portfolio and Project Management, versiones S4CORE 102, 103, EPPM 100, CPRXRPM 500_702, 600_740 y 610_740;
- SAP BusinessObjects Business Intelligence Platform (Monitoring Application), versiones 4.1, 4.2 y 4.3.

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 6 notas de seguridad y 1 actualización, siendo 1 de ellas de severidad crítica y 6 medias.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 1 vulnerabilidad de falta de comprobación de autorización;
- 4 vulnerabilidades de divulgación de información;
- 1 vulnerabilidad de CSRF (*Cross-Site Request Forgery*);
- 1 vulnerabilidad de XSS (*Cross-Site Scripting*);
- 2 vulnerabilidades de otro tipo.

La nota de seguridad más destacada se refiere a:

- SAP ha publicado la actualización de la versión compatible de Google Chromium para SAP Business Client, aunque la versión soportada todavía no soluciona las vulnerabilidades CVE-2019-13720 y CVE-2019-13721 publicadas por Google. Además, en el caso de que la vulnerabilidad CVE-2019-13720 estuviese siendo explotada, los sistemas SAP podrían verse afectados indirectamente a través de equipos cliente infectados conectados a la misma red. La próxima actualización podría mitigar sus efectos.

Para el resto de vulnerabilidades, se han reservado los siguientes identificadores: CVE-2019-0402, CVE-2019-0395, CVE-2019-0405, CVE-2019-0403, CVE-2019-0404, CVE-2019-0399 y CVE-2019-0398. El identificador CVE-2019-0325 está reservado.

Etiquetas: Actualización, SAP, Vulnerabilidad

Vulnerabilidad en Spectrum Scale de IBM

Fecha de publicación: 11/12/2019

Importancia: Alta

Recursos afectados:

IBM Spectrum Scale, versiones 5.0.0.0 - 5.0.4.0 y 4.2.0.0 - 4.2.3.18.

Descripción:

IBM ha identificado una vulnerabilidad de seguridad en IBM Spectrum Scale que podría permitir a un atacante remoto autenticado, ejecutar comandos arbitrarios en el sistema.

Solución:

Aplicar las actualizaciones a la versión 5.0.4.1 o 4.2.3.19.

Detalle:

Mediante el envío de una solicitud, especialmente diseñada, un atacante podría ejecutar comandos arbitrarios en el sistema. Se ha reservado el identificador CVE-2019-4715 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de diciembre de 2019

Fecha de publicación: 11/12/2019

Importancia: Crítica

Recursos afectados:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Office, Microsoft Office Services y Web Apps,
- SQL Server,
- Visual Studio,
- Skype for Business.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft correspondiente al mes de noviembre consta de 35 vulnerabilidades, 7 clasificadas como críticas y 28 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de información de la instalación de las mismas actualizaciones, se informa de los distintos métodos para llevarlas a cabo.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- divulgación de información,
- escalada de privilegios,
- denegación de servicio,
- ejecución remota de código,
- omisión de característica de seguridad,
- suplantación de identidad.

Etiquetas: Actualización, Microsoft, Windows

Múltiples vulnerabilidades en Xen

Fecha de publicación: 12/12/2019

Importancia: Alta

Recursos afectados:

- Todas las versiones de Xen.
- Citrix Hypervisor 8.0 y anteriores.
- Citrix XenServer 7.6.
- Citrix XenServer 7.1 LTSR CU2.
- Citrix XenServer 7.0.

Descripción:

Xen ha descubierto siete vulnerabilidades que afectan a sus productos. Un atacante remoto podría causar un cierre inesperado, generar una condición de denegación de servicio (DoS), escalar privilegios o divulgar información.

Solución:

Xen ha publicado una serie de actualizaciones que mitigan las vulnerabilidades.

Para más información, consultar el apartado Referencias.

Detalle:

Las vulnerabilidades detectadas podrían permitir a un atacante realizar:

- Cierre inesperado,
- generar una condición de denegación de servicio (DoS),
- escalada de privilegios.
- divulgación de información.

Se han reservado los identificadores CVE-2019-14607, CVE-2019-19577, CVE-2019-19578, CVE-2019-19580, CVE-2019-19581, CVE-2019-19582, CVE-2019-19583 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad 5.3.1 para WordPress

Fecha de publicación: 13/12/2019

Importancia: Alta

Recursos afectados:

WordPress, versiones 5.3 y anteriores.

Descripción:

Esta versión de seguridad y mantenimiento incluye 46 correcciones y mejoras. Además, agrega una serie de correcciones de seguridad.

Solución:

Ha sido publicada la versión 5.3.1 del gestor de contenidos, WordPress, para solucionar dichas vulnerabilidades, disponible desde su página de descarga.

Detalle:

Las correcciones de seguridad solucionan las siguientes vulnerabilidades:

- Un usuario no privilegiado podría enviar un mensaje a través de la API REST.
- *Cross-site scripting* (XSS) que podría ser almacenado en enlaces bien creados.
- Realizar *hardening* en *wp_kses_bad_protocol()* para asegurarse de que reconoce el atributo "dos puntos".
- XSS persistente usando contenido del editor de bloques.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en XtremIO de Dell EMC

Fecha de publicación: 17/12/2019

Importancia: Crítica

Recursos afectados:

Dell EMC XtremIO X2 XMS, versiones anteriores a la 6.3.0.

Descripción:

Lukasz Plonka ha identificado 3 vulnerabilidades, una de ellas con severidad crítica y las otras de severidad media, en el producto XtremIO de Dell EMC. La explotación de estas vulnerabilidades permitiría a un atacante remoto comprometer el sistema afectado.

Solución:

Actualizar Dell EMC XtremIO XMS a la versión 6.3.0 o posterior.

Detalle:

- La vulnerabilidad de severidad crítica podría permitir a un atacante con acceso remoto y nivel bajo de privilegios explotar una vulnerabilidad, de tipo XSS (*Cross-Site Scripting*) almacenado, y guardar código HTML o JavaScript malicioso en los campos de aplicación. Cuando los usuarios acceden a la página inyectada a través de sus navegadores, el código malicioso puede ser ejecutado por el navegador en el contexto de la aplicación web vulnerable. Se ha reservado el identificador CVE-2019-18578 para esta vulnerabilidad.
- Las vulnerabilidades de severidad media:
  - Se ha identificado una vulnerabilidad de divulgación de información en la que las contraseñas de los usuarios del sistema operativo se registran en archivos locales. Un atacante local, con acceso a los archivos de registro, puede usar las contraseñas expuestas para acceder a XtremIO con los privilegios del usuario comprometido. Se ha reservado el identificador CVE-2019-18576 para esta vulnerabilidad.
  - Una vulnerabilidad de asignación de permisos incorrecta permitiría a un atacante local, con privilegios *xinstall* en XtremIO, obtener acceso de *root* en caso de ser explotada. Se ha reservado el identificador CVE-2019-18577 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.14

Fecha de publicación: 18/12/2019

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones desde la 2.5.0, hasta la 3.9.13.

Descripción:

Joomla! ha publicado una nueva versión que soluciona dos vulnerabilidades de criticidad baja en su núcleo, de los tipos divulgación de ruta e inyección SQL.

Solución:

Actualizar a la versión 3.9.14.

Detalle:

- Se ha detectado una vulnerabilidad de falta de comprobación de acceso en los archivos del *framework* que podría dar lugar a una revelación de la ruta en la que se sitúan. Se ha asignado el identificador CVE-2019-19845 para esta vulnerabilidad.
- Una falta de validación de los parámetros de configuración utilizados en las consultas SQL permitiría realizar ataques de tipo inyección SQL. Se ha asignado el identificador CVE-2019-19846 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad en Citrix Application Delivery Controller y Citrix Gateway

Fecha de publicación: 18/12/2019

Importancia: Crítica

Recursos afectados:

- Citrix ADC y Citrix Gateway, versión 13.0, todas las *builds* con soporte;
- Citrix ADC y NetScaler Gateway, versión 12.1, todas las *builds* con soporte;
- Citrix ADC y NetScaler Gateway, versión 12.0, todas las *builds* con soporte;
- Citrix ADC y NetScaler Gateway, versión 11.1, todas las *builds* con soporte;
- Citrix NetScaler ADC y NetScaler Gateway, versión 10.5, todas las *builds* con soporte.

Descripción:

Se ha publicado una vulnerabilidad en productos Citrix que podría permitir a un atacante la ejecución arbitraria de código.

Solución:

Citrix publicará una actualización próximamente, mientras tanto, es posible aplicar las medidas de mitigación disponibles en el documento: pasos de mitigación para CVE-2019-19781.

Detalle:

Una vulnerabilidad en Citrix Application Delivery Controller (ADC) y Citrix Gateway podría permitir a un atacante, no autenticado, la ejecución arbitraria de código. Se ha reservado el identificador CVE-2019-19781 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en routers Archer de TP-Link

Fecha de publicación: 18/12/2019

Importancia: Alta

Recursos afectados:

- Archer C5 V4,
- Archer MR200v4,
- Archer MR6400v4,
- Archer MR400v3.

Descripción:

TP-Link ha descubierto una vulnerabilidad de criticidad alta que afecta a algunos dispositivos de su gama Archer. Un atacante remoto podría omitir la autenticación y tomar el control del dispositivo.

Solución:

TP-Link ha publicado actualizaciones que solucionan la vulnerabilidad de los productos afectados.

- Archer C5 V4,
- Archer MR200v4,
- Archer MR6400v4,
- Archer MR400v3.

Detalle:

La vulnerabilidad reside a la hora enviar un paquete HTTP, específicamente diseñado, que siempre es aceptado por el router, y permite realizar modificaciones en el dispositivo. Un atacante remoto podría explotar esta vulnerabilidad para tomar el control del dispositivo con permisos de administración (*root*). Se ha reservado el identificador CVE-2019-7405 para esta vulnerabilidad

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad en Planning Analytics de IBM

Fecha de publicación: 18/12/2019

Importancia: Crítica

Recursos afectados:

IBM Planning Analytics, versiones desde 2.0.0, hasta 2.0.8.

Descripción:

IBM ha publicado una vulnerabilidad de sobreescritura de configuración que podría permitir a un atacante acceder como administrador.

Solución:

IBM ha publicado la versión 2.0.9 para solucionar esta vulnerabilidad.

Detalle:

IBM Planning Analytics es vulnerable a una sobreescritura de configuración que podría permitir a un atacante, no autenticado, iniciar sesión como "admin" y, a continuación, ejecutar código como *root* o SYSTEM a través de secuencias de comandos TM1. Se ha reservado el identificador CVE-2019-4716 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos TIBCO

Fecha de publicación: 18/12/2019

Importancia: Alta

Recursos afectados:

- TIBCO Spotfire Analyst, versiones:
  - 7.11.1 y anteriores;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.4.0, 10.5.0 y 10.6.0.
- TIBCO Spotfire Analytics Platform para AWS Marketplace, versión 10.6.0;
- TIBCO Spotfire Deployment Kit, versiones 7.11.1 y anteriores;
- TIBCO Spotfire Desktop, versiones:
  - 7.11.1 y anteriores;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.4.0, 10.5.0 y 10.6.0.
- TIBCO Spotfire Desktop Language Packs, versión 7.11.1 y anteriores;
- TIBCO Spotfire Server, versiones:
  - 7.11.7 y anteriores;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.4.0, 10.5.0 y 10.6.0.
- Componentes:
  - visualizaciones;
  - capa de acceso a los datos;
  - librería de Spotfire.

Descripción:

TIBCO ha detectado tres vulnerabilidades de severidad alta. Un atacante remoto, no autenticado, podría ejecutar código, exponer credenciales para fuentes de datos compartidas o realizar XSS reflejado.

Solución:

- TIBCO Spotfire Analyst y TIBCO Spotfire Desktop:
  - para versión 7.11.1 y anteriores, actualizar a 7.11.2 o superiores;
  - para versiones 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1 y 10.3.2, actualizar a 10.3.3 o superiores;
  - para versiones 10.4.0, 10.5.0 y 10.6.0, actualizar a 10.6.1 o superiores.
- TIBCO Spotfire Analytics Platform para AWS Marketplace: actualizar a 10.6.1 o superiores;
- TIBCO Spotfire Deployment Kit: actualizar a 7.11.2 o superiores;
- TIBCO Spotfire Desktop Language Packs, actualizar a 7.11.2 o superiores;
- TIBCO Spotfire Server:
  - para versión 7.11.7 y anteriores, actualizar a 7.11.8 o superiores;
  - para versiones 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3 y 10.3.4, actualizar a 10.3.5 o superiores;
  - para versiones 10.4.0, 10.5.0 y 10.6.0, actualizar a 10.6.1 o superiores.

Detalle:

- Se ha identificado una vulnerabilidad que podría permitir a un atacante, con privilegios, modificar archivos DXP en la librería *Spotfire* para ejecutar código de manera remota en la cuenta de otros usuarios con acceso al sistema. Se ha asignado el identificador CVE-2019-17334 para esta vulnerabilidad.
- Un atacante podría acceder a información que permitiría la obtención de las credenciales utilizadas para acceder a las fuentes de datos de *Spotfire*. Únicamente cuando las credenciales NTLM o de un perfil están en uso se puede explotar esta vulnerabilidad. Se ha asignado el identificador CVE-2019-17336 para esta vulnerabilidad.
- Una vulnerabilidad de tipo XSS reflejado podría permitir a un atacante obtener acceso administrativo total a la interfaz web de los productos afectados. Se ha asignado el identificador CVE-2019-17337 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ejecución remota de código en el protocolo WebDAV utilizado por Microsoft Windows

Fecha de publicación: 19/12/2019

Importancia: Alta

Recursos afectados:

Clientes de Microsoft Windows que usen el protocolo WebDAV.

Descripción:

Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en los equipos afectados de Microsoft Windows.

Solución:

Dada la naturaleza de la vulnerabilidad, la única estrategia de mitigación destacada es restringir la interacción con el servicio a máquinas de confianza.

Detalle:

El fallo específico se encuentra en el manejo de las rutas de WebDAV, una extensión del protocolo HTTP que permite a los clientes realizar operaciones remotas de creación de contenido web. Una ruta WebDAV, específicamente diseñada, puede desencadenar la ejecución de una llamada de sistema compuesto por una cadena suministrada por el usuario. Un atacante remoto puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario actual.

Etiquetas: 0day, Vulnerabilidad

Múltiples vulnerabilidades en el core de Drupal

Fecha de publicación: 19/12/2019

Importancia: Alta

Recursos afectados:

- 7.x,
- 8.8.x,
- 8.7.x

Descripción:

El equipo de seguridad de Drupal ha detectado múltiples vulnerabilidades en el core que, entre otros, podrían permitir a un atacante la denegación del servicio, saltarse las protecciones del archivo *.htaccess* o acceder a elementos multimedia protegidos.

Solución:

Actualizar a las versiones 7.69, 8.8.1 y 8.7.11.

Detalle:

- Existen múltiples vulnerabilidades de severidad alta cuando Drupal está configurado para permitir que los archivos.tar,.tar.gz,.bz2 o.tlz se carguen y procesen, debido a una vulnerabilidad en la biblioteca de terceros *Archive_Tar*.
- El módulo de biblioteca multimedia no restringe suficientemente el acceso a elementos multimedia en determinadas configuraciones.
- La función *file_save_upload()* del núcleo de Drupal 8 no elimina el punto inicial y final ('.') de los nombres de archivo. Los usuarios con la capacidad de subir archivos con cualquier extensión junto con los módulos contribuidos pueden aprovechar esta vulnerabilidad para subir archivos de sistema como *.htaccess*, evitando las protecciones ofrecidas por el archivo *.htaccess* predeterminado de Drupal.
- Acceder al archivo *install.php* puede causar que los datos de la caché se corrompan y que el portal se vea afectado hasta que se reconstruyan las mismas.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de XSS en Unisphere para PowerMax de Dell EMC

Fecha de publicación: 20/12/2019

Importancia: Crítica

Recursos afectados:

Dell EMC Unisphere paraPowerMax, versiones anteriores a 9.1.0.9.

Descripción:

El investigador Tomasz Stachowicz, en colaboración con Dell EMC, ha detectado una vulnerabilidad de severidad crítica. Un atacante remoto, autenticado, podría ejecutar código arbitrario en el sistema.

Solución:

Actualizar Dell EMC Unsiphere para PowerMax a la versión 9.1.0.9 o posterior.

Detalle:

Una vulnerabilidad de tipo *Cross-site-scripting* (XSS) existente en el software, podría permitir a un atacante remoto, autenticado, inyectar código JavaScript en el sistema y afectar a otras sesiones de usuario. Se ha reservado el identificador CVE-2019-18588 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de restricción inadecuada en Palo Alto PAN-OS

Fecha de publicación: 20/12/2019

Importancia: Crítica

Recursos afectados:

PAN-OS 9.0, versiones anteriores a 9.0.5-h3 en PA-7000 Series, con SMC (*Switch Management Card*) de segunda generación y LFC (*Log Forwarding Card*) instalado y configurado.

Descripción:

Ayad (Ed) Sleiman y su equipo, de KAUST, han descubierto y reportado una vulnerabilidad de restricción inadecuada en las comunicaciones a LFC.

Solución:

La versión 9.0.5-h3 y posteriores, y la actualización de contenido 8218-5815, solucionan esta vulnerabilidad.

Detalle:

Una vulnerabilidad de restricción indebida del canal de comunicación en los *endpoints* previstos, podría permitir a un atacante, con acceso a la red del LFC, obtener acceso con privilegios de *root* a PAN-OS. Se ha reservado el identificador CVE-2019-17440 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Watson Studio Local de IBM

Fecha de publicación: 23/12/2019

Importancia: Alta

Recursos afectados:

- IBM Watson Studio Local, versión 1.2.3;

Descripción:

IBM ha publicado múltiples vulnerabilidades de severidad alta en Watson Studio Local.

Solución:

Aplicar la siguiente actualización.

Detalle:

- Una vulnerabilidad que involucraba enlaces simbólicos, permitía el acceso arbitrario al directorio de usuarios de Watson Studio Local.
- La falta de validación de los datos de entrada ofrece un vector de ataque en varias llamadas a la API.
- Se eliminó el soporte del antiguo protocolo SSL.

Etiquetas: Actualización, IBM, Vulnerabilidad

Fuga de memoria en el proceso tmrouted en BIG-IP de F5

Fecha de publicación: 26/12/2019

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM), versiones:
  - 15.0.0 - 15.0.1;
  - 14.1.0 - 14.1.2;
  - 14.0.0 - 14.0.1;
  - 13.1.0 - 13.1.3;

- 12.1.0 - 12.1.5.

Descripción:

Una vulnerabilidad en los sistemas BIG-IP, con licencia *Routing* y configurado con *Multicast Forwarding Cache* (MFC), podría permitir a un atacante provocar la denegación del servicio.

Solución:

Actualizar a las versiones:

- 15.1.0,
- 14.1.2.1,
- 14.0.1.1,
- 13.1.3.2.

Detalle:

Un sistema BIG-IP, con licencia *Routing* y configurado con *Multicast Forwarding Cache* (MFC), podría experimentar una fuga de memoria en el proceso *tmrouted*, agotar los recursos del sistema y reiniciarlo. Esto podría permitir a un atacante causar la denegación del servicio. Se ha asignado el identificador CVE-2019-6681 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de inyección de parámetros en IBM Spectrum Scale

Fecha de publicación: 26/12/2019

Importancia: Alta

Recursos afectados:

IBM Elastic Storage Server, versiones:

- desde 5.3.0, hasta 5.3.4.1;
- desde 5.0.0, hasta 5.2.7.0;
- desde 4.5.0, hasta 4.6.0.0;
- desde 4.0.0, hasta 4.0.6.0.

Descripción:

IBM Elastic Storage Server está afectado por una vulnerabilidad en IBM Spectrum Scale, donde se pueden obtener privilegios de *root* inyectando parámetros en los archivos *setuid*.

Solución:

- Para IBM Elastic Storage Server, versiones desde 5.0.0, hasta 5.3.4.1, actualizar a la versión 5.3.4.2;
- Para IBM Elastic Storage Server, versiones desde 5.0.0, hasta 5.2.7.0, actualizar a la versión 5.2.8;
- Si no es posible actualizar a las versiones 5.3.2.0 o 5.2.5 de IBM Elastic Storage Server, contactar con IBM Service para obtener un *efix*:
  - para IBM Elastic Storage Server, versiones desde 5.3.0.0, hasta 5.3.4.1, aplicar APAR IJ18477;
  - para IBM Elastic Storage Server, versiones desde 5.0.0.0, hasta 5.2.7.0, aplicar APAR IJ18518;
  - para IBM Elastic Storage Server, versiones desde 4.0.0, hasta 4.6.0, aplicar APAR IJ18518.

Detalle:

Se ha identificado una vulnerabilidad en todos los niveles de IBM Spectrum Scale, versiones desde 5.0.0.0, hasta 5.0.3.2 y desde 4.2.0.0, hasta 4.2.3.17, que podría permitir que un atacante local obtuviera privilegios de *root* inyectando parámetros en los archivos *setuid*. Se ha asignado el identificador CVE-2019-4558 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad