
# Boletín de noviembre de 2019

## Avisos Técnicos

## Vulnerabilidad de XSS en BIG-IP TMUI de F5

**Fecha de publicación:** 04/11/2019

**Importancia:** Alta

**Recursos afectados:**

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM y WebAccelerator), versiones:
  - desde 13.1.0, hasta 13.1.3;
  - desde 12.1.0, hasta 12.1.5;
  - desde 11.5.2, hasta 11.6.5.

**Descripción:**

The Tarantula Team ha descubierto una vulnerabilidad de *cross-site scripting* (XSS) reflejado en una página no revelada en el componente *Traffic Management User Interface* (TMUI) del producto BIG-IP , también conocido como la utilidad de configuración de BIG-IP.

**Solución:**

Actualizar BIG-IP a la versión 14.0.0.

**Detalle:**

Un atacante puede explotar esta vulnerabilidad utilizando una URL, especialmente diseñada, para realizar un ataque XSS reflejado en una página no revelada de las páginas de seguridad de TMUI. Se ha asignado el identificador CVE-2019-6657 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

## Múltiples vulnerabilidades en Xen

**Fecha de publicación:** 04/11/2019

**Importancia:** Alta

**Recursos afectados:**

- Xen, versiones 4.6 y posteriores;
- Xen, versiones de 32 bit, desde la versión 3.2;
- Xen, todos los sistemas x86, con invitados PV sin confianza;
- los sistemas Xen en los que los huéspedes tengan acceso directo a los dispositivos físicos.
- Xen, todos los sistemas ARM;
- Citrix Hypervisor, versión 8.0 y anteriores.

**Descripción:**

Se han publicado varias vulnerabilidades en Xen que podrían permitir la denegación del servicio, escalada de privilegios o corrupción de datos.

**Solución:**

Se recomienda aplicar los parches publicados para resolver estas vulnerabilidades. Para más información, consultar la sección de *Referencias*.

**Detalle:**

- La interpretación de los parámetros de entrada con formato incorrecto provoca un fallo en la función

*hypercall_create_continuation()* que ocasiona el cierre inesperado de Xen. Se ha asignado el identificador CVE-2019-18420 para esta vulnerabilidad.
- La emulación del modo de usuario invitado de 32 bits podría permitir a un atacante su instalación y posterior utilización de descriptores a su elección, lo que podría provocar la escalada de privilegios. Se ha asignado el identificador CVE-2019-18425 para esta vulnerabilidad.
- Un atacante podría ganar acceso de escritura en las tablas de página en uso para escalar privilegios. Se ha asignado el identificador CVE-2019-18421 para esta vulnerabilidad.
- Una hiperllamada especialmente diseñada, junto con el acceso a una dirección, a través de hipervínculo o acceso directo, que eluda las comprobaciones de control, podría permitir a un atacante causar el cierre inesperado del hipervisor, resultando en la denegación del servicio. Se ha asignado el identificador CVE-2019-18423 para esta vulnerabilidad.
- Cuando el dominio huésped se cierra o el dispositivo se asigna de nuevo al dominio dom0, un dominio no confiable con acceso a un dispositivo físico podría acceder a la memoria del sistema para leer o escribir, lo que provocaría la escalada de privilegios. Se ha asignado el identificador CVE-2019-18424 para esta vulnerabilidad.
- Cuando ocurre una excepción en un sistema ARM, algunas interrupciones se habilitan incondicionalmente durante la entrada de excepciones, esto podría permitir a un atacante la corrupción de los datos, denegación del servicio o escalada de privilegios. Se ha asignado el identificador CVE-2019-18422 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Actualización de seguridad de Joomla! 3.9.13

**Fecha de publicación:** 06/11/2019

**Importancia:** Baja

**Recursos afectados:**

Joomla! CMS, versiones desde la 3.2.0, hasta la 3.9.12.

**Descripción:**

Joomla! ha publicado una nueva versión que soluciona dos vulnerabilidades de criticidad baja en su núcleo, de los tipos *cross-site request forgery* (CSRF) y divulgación de ruta.

**Solución:**

Actualizar a la versión 3.9.13.

**Detalle:**

- Una falta de comprobación en el *token* en *com_template* podría causar una vulnerabilidad del tipo CSRF. Se ha asignado el identificador CVE-2019-18650 para esta vulnerabilidad.
- Una falta de comprobación de acceso en los archivos de mapeado de *phputf8* podría permitir una divulgación de ruta. Se ha asignado el identificador CVE-2019-18674 para esta vulnerabilidad.

**Etiquetas:** Actualización, CMS, Vulnerabilidad

---

# Múltiples vulnerabilidades en Workstation y Fusion de WMware

**Fecha de publicación:** 13/11/2019

**Importancia:** Alta

**Recursos afectados:**

- VMware Workstation Pro / Player, versiones anteriores a la 15.5.1,
- VMware Fusion Pro / Fusion, versiones anteriores a la 15.5.1.

**Descripción:**

VMware ha detectado tres vulnerabilidades, dos con criticidades altas y una media. Un atacante remoto podría generar una condición de denegación de servicio, revelar información sensible o ejecución de código.

**Solución:**

VMware ha publicado actualizaciones que solucionan las vulnerabilidades en función del producto afectado.

- Actualizar VMware Workstation Pro a la versión 15.5.1,
- Actualizar VMware Workstation Player a la versión 15.5.1,
- Actualizar VMware Fusion a la versión 15.5.1.

**Detalle:**

Las vulnerabilidades con criticidad alta son:

- Una vulnerabilidad de escritura fuera de límites en el adaptador de red virtual e1000e podría permitir a un atacante remoto la ejecución de código en el *host* desde la máquina virtual o generar una condición de denegación de servicio en la máquina virtual. Se ha reservado el identificador CVE-2019-5541 para esta vulnerabilidad.
- *vmnetdhcp* contiene una vulnerabilidad a través de la que un atacante remoto en la máquina virtual podría obtener información de la memoria de los procesos del *host*, y utilizarla para revelar información sensible del *host*. Se ha reservado el identificador CVE-2019-5540 para esta vulnerabilidad.

A la vulnerabilidad de criticidad media se le ha reservado el identificador CVE-2019-5542.

**Etiquetas:** Actualización, VMware, Vulnerabilidad

# Cross-site scripting (XSS) en TIBCO EBX

**Fecha de publicación:** 13/11/2019

**Importancia:** Alta

**Recursos afectados:**

- El servidor web de las siguientes versiones de TIBCO EBX:
  - 5.8.1.fixR y anteriores
  - 5.9.3, 5.9.4, 5.9.5 y 5.9.6
- En el interfaz web del Digital Asset Manager de las siguientes versiones de los complementos (Add-ons) de TIBCO EBX:
  - 3.20.13 y anteriores
  - 4.1.0, 4.2.0, 4.2.1 y 4.2.2
- En el interfaz web del Data Exchange las siguientes versiones de los complementos (Add-ons) de TIBCO EBX:
  - 3.20.13 y anteriores
  - 4.1.0

**Descripción:**

TIBCO ha publicado 3 vulnerabilidades que afectan a varios de sus productos, que permitirían a un atacante realizar ataques cross-site scripting (XSS).

**Solución:**

TIBCO ha publicado actualizaciones de los sistemas afectados que abordan estos problemas:

- Las versiones 5.8.1.fixR y posteriores se actualizan a la versión 5.8.1.fixS o superior.
- Las versiones 5.9.3, 5.9.4, 5.9.5 y 5.9.6 se actualizan a la versión 5.9.7 o superior.
- Los complementos para el interfaz web del Digital Asset Manager versiones 3.20.13 y posteriores se actualizan a la versión 3.20.14 o superior.
- Los complementos para el interfaz web del Digital Asset Manager versiones 4.1.0, 4.2.0, 4.2.1 y 4.2.2 se actualizan a la versión 4.3.0 o superior.
- Los complementos para el interfaz web del Data Exchange versiones 3.20.13 y posteriores se actualizan a la versión 3.20.14 o superior.
- Los complementos para el interfaz web del Data Exchange versiones 4.1.0 se actualizan a la versión 4.2.0 o superior.

**Detalle:**

- La vulnerabilidad que afecta al servidor web podría permitir a usuarios autenticados realizar ataques XSS entre sitios almacenados, y a usuarios no autenticados realizar ataques de XSS entre sitios reflejados. Se ha asignado el identificador CVE-2019-17330 para esta vulnerabilidad.
- La vulnerabilidad que afecta a los complementos del interfaz web del Digital Asset Manager podría permitir a usuarios autenticados realizar ataques XSS entre sitios almacenados. Se ha asignado el identificador CVE-2019-17332 para esta vulnerabilidad.
- La vulnerabilidad que afecta a los complementos del interfaz web del Data Exchange podría permitir a usuarios autenticados realizar ataques XSS entre sitios almacenados. Se ha asignado el identificador CVE-2019-17331 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

# Múltiples vulnerabilidades en productos de Intel

**Fecha de publicación:** 13/11/2019

**Importancia:** Crítica

**Recursos afectados:**

- Intel Core:
  - desde la 2ª, hasta la 10ª generación de procesadores;
  - familia m;
  - familia X-series.
- Intel Pentium serie Gold;
- Intel Celeron:
  - serie G;
  - serie 5000.
- Intel Xeon:
  - Scalable;
  - familia E;
  - familia D;
  - familia W;
  - legacy.
- Intel Atom serie C;
- Intel Converged Security and Manageability Engine (CSME), Intel Active Management Technology (AMT), Intel Dynamic Application Loader (DAL) e Intel DAL software:
  - desde 11.0, hasta 11.8.65;
  - desde 11.10, hasta 11.11.65;
  - desde 11.20, hasta 11.22.65;
  - desde 12.0, hasta 12.0.35;
  - 13.0.0;
  - 14.0.0.
- Intel SPS:
  - desde SPS_E5_04.00.03.199.0, hasta SPS_E5_04.00.04.380.0;
  - desde SPS_SoC-X_04.00.04.051.0, hasta SPS_SoC-X_04.00.04.085.0;
  - desde SPS_SoC-A_04.00.03.065.0, hasta SPS_SoC-A_04.00.04.180.0;
  - desde SPS_E3_04.01.03.021.0, hasta SPS_E3_04.01.04.053.0.
- Intel Trusted Execution Engine (TXE):

    - desde 3.0, hasta 3.1.65;
    - desde 4.0, hasta 4.0.15.
- Intel Ethernet 700 Series Controller:
    - versión de firmware anterior a 7.0;
    - versión de software anterior a 24.0.
- Intel WIFI Drivers e Intel PROSet/Wireless WiFi Software, versiones anteriores a 21.40 para los siguientes productos:
    - Intel Wi-Fi 6 AX201 y AX200;
    - Intel Wireless-AC 9560, 9462, 9461 y 9260;
    - Intel Dual Band Wireless-AC 8265, 8260 y 3168;
    - familia Intel Wireless 7265 (Rev D);
    - Intel Dual Band Wireless-AC 3165.
- Intel SGX SDK para Windows, versiones:
    - 2.4.100.51291 y anteriores;
    - 2.3.101.50222;
    - 2.3.100.49777.
- Intel SGX SDK para Linux, versiones:
    - 2.6.100.51363 y anteriores;
    - 2.5.100.49891;
    - 2.4.100.48163;
    - 2.3.100.46354;
    - 2.2.100.45311.
- Intel Server Boards, versiones: BBS2600BPB, BBS2600BPQ, BBS2600BPS, BBS2600BPBR, BBS2600BPQR, BBS2600BPSR, S2600WF0, S2600WFQ, S2600WFT, S2600WF0R, S2600WFQR, S2600WFTR, S2600STB, S2600STQ, S2600STBR, S2600STQR, BBS2600STB, BBS2600STQ, BBS2600STBR y BBS2600STQR;
- Intel Compute Modules, versiones: HNS2600BPB, HNS2600BPQ, HNS2600BPS, HNS2600BPB24, HNS2600BPQ24, HNS2600BPS24, HNS2600BPBLC, HNS2600BPBLC24, HNS2600BPBR, HNS2600BPBRX, HPCHNS2600BPBR, HNS2600BPQR, HPCHNS2600BPQR, HNS2600BPSR, HPCHNS2600BPSR, HNS2600BPB24R, HNS2600BPB24RX, HNS2600BPQ24R, HNS2600BPS24R, HNS2600BPBLCR, HNS2600BPBLC24R, S9256WK1HLC, S9248WK1HLC, S9232WK1HLC, S9248WK2HLC, S9232WK2HLC, S9248WK2HAC y S9232WK2HAC;
- Intel Server Systems, versiones: R1304WF0YS, R1304WFTYS, R1208WFTYS, R2308WFTZS, R2208WF0ZS, R2208WFTZS, R2208WFQZS, R2312WF0NP, R2312WFTZS, R2312WFQZS, R2224WFQZS, R2224WFTZS, R1208WFTYSR, HPCR1208WFTYSR, R1304WF0YSR, HPCR1304WF0YSR, R1304WFTYSR, HPCR1304WFTYSR, R2208WFTZSR, R2208WFTZSRX, HPCR2208WFTZSR, HPCR2208WFTZSRX, R2208WF0ZSR, HPCR2208WF0ZSR, R2224WFTZSR, HPCR2224WFTZSR, R2308WFTZSR, HPCR2308WFTZSR, R2312WFTZSR, HPCR2312WFTZSR, R2312WF0NPR, HPCR2312WF0NPR, R2208WFQZSR, HPCR2208WFQZSR, R1208WFQYSR y HPCR1208WFQYSR.

Estas vulnerabilidades afectan a fabricantes como:

- Xen: sistemas que estén ejecutando todas las versiones de Xen (procesadores x86 basados en Intel);
- Citrix
    - Citrix Hypervisor, versión 8.0 y anteriores;
    - Citrix ADC y Citrix Gateway, las siguientes series MPX/SDX:
        - 8900;
        - 14000-40G/14000-40S/14000-40C;
        - 15000-25G/15000-50G;
        - 25000-40G;
        - 26000/26000-50G.
- Dell: Dell EMC Servers y Dell EMC Networking Virtual Edge Platform 4600 (VEP 4600).

**Descripción:**

Intel ha publicado 12 avisos de seguridad en su centro de seguridad de productos, 2 de severidad crítica, 8 de severidad alta y 2 de severidad media. Estas vulnerabilidades también afectan a otros fabricantes que utilizan componentes de Intel en sus propios productos.

**Solución:**

Actualizar a la última versión del producto.

**Detalle:**

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- denegación de servicio;
- escalada de privilegios;
- divulgación de información.

Se han reservado los siguientes identificadores: CVE-2018-12207, CVE-2019-0123, CVE-2019-0124, CVE-2019-0152, CVE-2019-0151, CVE-2019-0169, CVE-2019-11132, CVE-2019-11147, CVE-2019-11105, CVE-2019-11088, CVE-2019-11131, CVE-2019-11104, CVE-2019-11097, CVE-2019-11103, CVE-2019-0131, CVE-2019-11090, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-11087, CVE-2019-11101, CVE-2019-11100, CVE-2019-11102, CVE-2019-11106, CVE-2019-11107, CVE-2019-11109, CVE-2019-11110, CVE-2019-11086, CVE-2019-11108, CVE-2019-11112, CVE-2019-0155, CVE-2019-11111, CVE-2019-14574, CVE-2019-14590, CVE-2019-14591, CVE-2019-11089, CVE-2019-11113, CVE-2019-0140, CVE-2019-0145, CVE-2019-0142, CVE-2019-0139, CVE-2019-0143, CVE-2019-0144, CVE-2019-0146, CVE-2019-0147, CVE-2019-0148, CVE-2019-0149, CVE-2019-0150, CVE-2019-11135, CVE-2019-11136, CVE-2019-11137, CVE-2019-11151, CVE-2019-11152, CVE-2019-11153, CVE-2019-11154, CVE-2019-11155, CVE-2019-11156, CVE-2019-14566, CVE-2019-14565, CVE-2019-11168, CVE-2019-11170, CVE-2019-11171, CVE-2019-11172, CVE-2019-11173, CVE-2019-11174, CVE-2019-11175, CVE-2019-11177, CVE-2019-11178, CVE-2019-11179, CVE-2019-11180, CVE-2019-11181 y CVE-2019-11182.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Actualización de seguridad de SAP de noviembre de 2019

**Fecha de publicación:** 13/11/2019

**Importancia:** Crítica

**Recursos afectados:**

- SAP Business Client, versión 6.5;

- SAP Diagnostic Agent (LM-Service), versión 7.20;
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), versiones 4.1 y 4.2;
- SAP Enable Now, versiones anteriores a la 1908;
- S4HANA Sales (S4CORE), versiones 1.0, 1.01, 1.02, 1.03 y 1.04;
- SAP Treasury and Risk Management (EA-FINSERV), versiones 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18 y 8.0;
- SAP NetWeaver Application Server Java (J2EE-Framework), versiones - 7.1, 7.2, 7.3, 7.31, 7.4 y 7.5;
- SAP Quality Management (S4CORE), versiones 1.0, 1.01, 1.02 y 1.03;
- SAP UI 700, versión 2.0;
- SAP NetWeaver AS Java, versiones 7.10, 7.20, 7.30, 7.31, 7.4 y 7.5;
- SAP Treasury and Risk Management (S4CORE), versiones 1.01, 1.02, 1.03 y 1.04;

**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 11 notas de seguridad y 4 actualizaciones, siendo 4 de ellas de severidad crítica, 1 alta, y 10 medias.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 1 vulnerabilidad de *SQL injection,*
- 1 vulnerabilidad de escalada de privilegios,
- 3 vulnerabilidades de inyección de comandos del sistema operativo,
- 1 vulnerabilidad de falta de comprobación de XML;
- 1 vulnerabilidad de comprobación de autorización;
- 1 vulnerabilidad de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Se han encontrado nuevos bypass múltiples sobre la lista blanca definida para Linux/Unix que podría permitir a un atacante eliminar, modificar o ejecutar comandos arbitrarios en el agente. Se ha asignado el identificador CVE-2019-0330 para esta vulnerabilidad.
- Se ha incluido una validación XML adicional en SAP Business Objects Business Intelligence Platform, ya que los documentos XML procedentes de fuentes no fiables no se filtraban correctamente para detectar contenido malicioso, lo que podía permitir a un atacante la divulgación de información o la denegación del servicio. Se ha reservado el identificador CVE-2019-0396 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2019-0385, CVE-2019-0386, CVE-2019-0384, CVE-2019-0389, CVE-2019-0382, CVE-2019-0393, CVE-2019-0390, CVE-2019-0388, CVE-2019-0391 y CVE-2019-0383.

**Etiquetas:** Actualización, SAP, Vulnerabilidad

---

# Ejecución remota de código en Cisco ASA y Cisco Firepower (FTD)

**Fecha de publicación:** 13/11/2019

**Importancia:** Alta

**Recursos afectados:**

Todas las versiones del software Cisco ASA y del software Cisco FTD.

**Descripción:**

Se ha descubierto una vulnerabilidad de ejecución remota de código que afecta a la implementación del intérprete Lua, integrado en el software de todas las versiones de Cisco ASA y Cisco Firepower (FTD).

**Solución:**

Cisco no ha publicado actualizaciones de software que aborden esta vulnerabilidad. Desde el fabricante tampoco se han aportado soluciones alternativas que permitan actualmente mitigar esta vulnerabilidad.

Desde INCIBE-CERT recomendamos que los usuarios tomen las siguientes medidas defensivas para minimizar el riesgo de explotación de esta vulnerabilidad:

- Minimizar la exposición de la red para todos los sistemas o dispositivos Cisco ASA y Cisco Firepower (FTD) y asegurar que no sean accesibles desde redes externas.
- Limitar a usuarios de confianza el acceso a los dispositivos con credenciales administrativas, así como evitar ejecutar archivos de fuentes desconocidas o que no sean de confianza.
- Implementar sistemas de detección de intrusos en la red para monitorear el tráfico de la red en busca de actividad maliciosa.

**Detalle:**

La vulnerabilidad descubierta se debe a restricciones insuficientes en las llamadas a funciones permitidas a través de la utilización de scripts Lua que pueden utilizar los usuarios con privilegios administrativos. Una explotación exitosa podría permitir al atacante activar una condición de desbordamiento de pila y ejecutar código arbitrario con privilegios de root en el sistema operativo Linux incluido en el dispositivo afectado.

En el caso de dispositivos Cisco ASA a través de scripts Lua, un usuario con privilegios administrativos puede definir las funciones Dynamic Access Policy (DAP) para gestión de atributos de control de acceso que se evalúan dinámicamente en el momento de establecer una sesión VPN.

En los dispositivos Cisco Firepower (FTD) se pueden utilizar los scripts Lua por parte de usuarios con privilegios administrativos para definir una lógica personalizada para identificar y filtrar el tráfico IP a través de la funcionalidad Custom Application Detectors integrada

en el Firepower Management Center (FMC).

**Etiquetas:** Actualización, Cisco, Linux, Vulnerabilidad

# Boletín de seguridad de Microsoft de noviembre de 2019

**Fecha de publicación:** 13/11/2019

**Importancia:** Crítica

**Recursos afectados:**

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge (Edge basado en HTML),
- ChakraCore,
- Microsoft Office y Microsoft Office Services y Web Apps,
- Open Source Software,
- Microsoft Exchange Server,
- Visual Studio,
- Azure Stack.

**Descripción:**

La publicación de actualizaciones de seguridad de Microsoft correspondiente al mes de noviembre consta de 75 vulnerabilidades, 13 clasificadas como críticas y 62 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:

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

**Etiquetas:** Actualización, Microsoft, Navegador, Windows

# Vulnerabilidad de denegación de servicio en BIG-IP de F5

**Fecha de publicación:** 15/11/2019

**Importancia:** Alta

**Recursos afectados:**

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones desde 14.0.0, hasta 14.1.0.1.

**Descripción:**

Los servidores virtuales BIG-IP, con TLS 1.3, activado podrían experimentar una denegación de servicio (DoS) debido a mensajes entrantes no revelados.

**Solución:**

Actualizar BIG-IP a las siguientes versiones:

- 15.0.0;
- 14.1.0.2.

**Detalle:**

Existe una vulnerabilidad en la recepción de los mensajes no revelados en los servidores virtuales BIG-IP que dispongan de TLS 1.3 habilitado. Un atacante remoto podría generar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-6659 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

# Vulnerabilidad de inyección CSV en UCD de IBM

**Fecha de publicación:** 15/11/2019

**Importancia:** Alta

**Recursos afectados:**

UCD - IBM UrbanCode Deploy.

**Descripción:**

Se ha publicado una vulnerabilidad de inyección CSV que podría permitir la generación de un archivo de descarga CSV malicioso.

**Solución:**

Actualizar a la versión 7.0.4.0 o posterior.

**Detalle:**

La inyección de código, especialmente diseñado, en el UCD podría permitir a un atacante generar un archivo de descarga CSV malicioso al ser abierto desde herramientas de terceros no parcheadas. Se ha reservado el identificador CVE-2019-4490 para esta vulnerabilidad.

**Etiquetas:** Actualización, IBM, Vulnerabilidad

---

# Múltiples vulnerabilidades en Moodle

**Fecha de publicación:** 18/11/2019

**Importancia:** Alta

**Recursos afectados:**

Las vulnerabilidades afectan a las siguientes versiones:

- desde la 3.7 a la 3.7.2,
- desde la 3.6 a la 3.6.6,
- desde la 3.5 a la 3.5.8,
- versiones anteriores sin soporte.

**Descripción:**

Se han publicado seis vulnerabilidades que afectan a la plataforma Moodle. Las dos de severidad más alta, podrían permitir llevar a cabo ataques de *Cross Site Scripting (XSS)* o comprometer la cuenta.

**Solución:**

Actualizar a las versiones 3.7.3, 3.6.7 y 3.5.9.

**Detalle:**

De las seis vulnerabilidades reportadas, cuatro son de criticidad baja y dos de criticidad alta, cuyo detalle es el siguiente:

- Vulnerabilidad de *Cross Site Scripting (XSS)* reflejado en algunos mensajes de error. Se ha reservado el identificador CVE-2019-14884 para esta vulnerabilidad.
- Algunos inicios de sesión de OAuth 2 podrían comprometer las cuentas. Se ha reservado el identificador CVE-2019-14880 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han reservado los siguientes identificadores: CVE-2019-14879, CVE-2019-14881, CVE-2019-14882 y CVE-2019-14883.

**Etiquetas:** Actualización, CMS, Vulnerabilidad

---

# Vulnerabilidad en Security Identy Manager de IBM

**Fecha de publicación:** 20/11/2019

**Importancia:** Alta

**Recursos afectados:**

ISIM (SS) versión 6.0.0

**Descripción:**

Se ha publicado una vulnerabilidad en Security Identy Manager de IBM.

**Solución:**

Actualizar a la versión 6.0.0.22-ISS-SIM-IF0001

**Detalle:**

IBM ha publicado una vulnerabilidad en IBM Security Identy Manager. Se ha reservado el identificador CVE-2019-4561 para esta vulnerabilidad.

**Etiquetas:** Actualización, IBM

---

# Múltiples vulnerabilidades en Cloud Pak System de IBM

**Fecha de publicación:** 21/11/2019

**Importancia:** Alta

**Recursos afectados:**

IBM Cloud Pak System, versión 2.3.0.

**Descripción:**

Se han identificado dos vulnerabilidades, ambas de severidad alta, en el producto Cloud Pak System de IBM.

**Solución:**

Actualizar Cloud Pak System a la versión 2.3.0.1.

**Detalle:**

- IBM Pure Application System podría permitir a un usuario autenticado con acceso local eludir la seguridad, debido a la falta de validación de entrada y, de esta manera, obtener acceso con privilegios de administrador. Se ha reservado el identificador CVE-2019-4240 para esta vulnerabilidad.
- IBM Pure Application System utiliza una configuración de bloqueo de cuenta inadecuada, que podría permitir a un atacante remoto realizar un ataque de fuerza bruta para obtener las credenciales de las cuentas. Se ha reservado el identificador CVE-2019-4096 para esta vulnerabilidad.

**Etiquetas:** Actualización, IBM, Vulnerabilidad

---

# Vulnerabilidad de inyección SQL en phpMyAdmin

**Fecha de publicación:** 25/11/2019

**Importancia:** Alta

**Recursos afectados:**

Versiones de phpMyAdmin anteriores a la 4.9.2, al menos tan antiguas como la 4.7.7.

**Descripción:**

William Desportes, del equipo de phpMyAdmin, ha descubierto una vulnerabilidad de inyección SQL.

**Solución:**

Actualizar a la versión 4.9.2 o superior, o aplicar el parche correspondiente.

**Detalle:**

Se reportó una vulnerabilidad en la que se puede utilizar un nombre de base de datos, especialmente diseñado para desencadenar un ataque de inyección SQL a través de una funcionalidad en el editor. Se ha asignado el identificador CVE-2019-18622 para esta vulnerabilidad.

**Etiquetas:** Actualización, PHP, Vulnerabilidad

---

# Vulnerabilidad de omisión de autenticación en BIG-IP de F5

**Fecha de publicación:** 26/11/2019

**Importancia:** Crítica

**Recursos afectados:**

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x:
  - 15.0.1.0.33.11-ENG Hotfix;
  - 15.0.1.0.48.11-ENG Hotfix.
- 14.x:
  - 14.1.0.3.0.79.6-ENG Hotfix;
  - 14.1.0.3.0.97.6-ENG Hotfix;
  - 14.1.0.3.0.99.6-ENG Hotfix;
  - 14.1.0.5.0.15.5-ENG Hotfix;
  - 14.1.0.5.0.36.5-ENG Hotfix;
  - 14.1.0.5.0.40.5-ENG Hotfix;
  - 14.1.0.6.0.11.9-ENG Hotfix;
  - 14.1.0.6.0.14.9-ENG Hotfix;
  - 14.1.0.6.0.68.9-ENG Hotfix;
  - 14.1.0.6.0.70.9-ENG Hotfix;
  - 14.1.2.0.11.37-ENG Hotfix;
  - 14.1.2.0.18.37-ENG Hotfix;

- 14.1.2.0.32.37-ENG Hotfix;
- 14.1.2.1.0.46.4-ENG Hotfix;
- 14.1.2.1.0.14.4-ENG Hotfix;
- 14.1.2.1.0.16.4-ENG Hotfix;
- 14.1.2.1.0.34.4-ENG Hotfix;
- 14.1.2.1.0.97.4-ENG Hotfix;
- 14.1.2.1.0.99.4-ENG Hotfix;
- 14.1.2.1.0.105.4-ENG Hotfix;
- 14.1.2.1.0.111.4-ENG Hotfix;
- 14.1.2.1.0.115.4-ENG Hotfix;
- 14.1.2.1.0.122.4-ENG Hotfix.

**NOTA**: esta vulnerabilidad afecta únicamente a los *hotfixes* de BIG-IP Engineering obtenidos del soporte de F5. Las versiones *major*, *minor*, o *maintenance* obtenidas de la web de descargas de F5 no se ven afectadas.

**Descripción:**

Las configuraciones BIG-IP que utilizan Active Directory, LDAP o Client Certificate LDAP para la autenticación de gestión con varios servidores están expuestas a esta vulnerabilidad, que permite una omisión de autenticación que puede causar un compromiso total del sistema.

**Solución:**

No hay actualización disponible para solucionar la vulnerabilidad. Para mitigar esta vulnerabilidad, F5 recomienda aplicar estas medidas:

- Deshabilitar cualquier autenticación LDAP remota para usuarios remotos.
- Configurar la autenticación LDAP remota con un único servidor de autenticación.
- Implementar controles de acceso estrictos basados en la dirección IP de origen de la interfaz de gestión del sistema BIG-IP.

**Detalle:**

Los usuarios remotos que se autentican en el sistema BIG-IP utilizando LDAP, Directorio Activo o Client Certificate LDAP, pueden iniciar sesión con credenciales incorrectas, pudiendo comprometer completamente el sistema BIG-IP. Se ha reservado el identificador CVE-2019-6675 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en productos F5

**Fecha de publicación:** 27/11/2019

**Importancia:** Alta

**Recursos afectados:**

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:
  - 15.0.0 - 15.0.1;
  - 14.1.0 - 14.1.2;
  - 14.0.0 - 14.0.1;
  - 13.1.0 - 13.1.3.1;
  - 12.1.0 - 12.1.5;
  - 11.5.1 - 11.6.5.
- Enterprise Manager, versión 3.1.1.
- BIG-IQ Centralized Management, versiones:
  - 6.0.0;
  - 5.2.0 - 5.4.0.
- F5 iWorkflow, versión 2.3.0.

**Descripción:**

Se han publicado múltiples vulnerabilidades en productos F5 que podrían permitir a un atacante configurar el proxy para interceptar el tráfico, denegar el servicio o acceder a los archivos de la cuenta *root*.

**Solución:**

Actualizar a las siguientes versiones:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:
  - 15.0.1.1;
  - 14.1.2.1;
  - 14.0.1.1;
  - 13.1.3.2;
  - 12.1.5;
  - 11.6.5.1;
- BIG-IQ Centralized Management, versión 6.1.00

**Detalle:**

- Con acceso al *token* de autenticación, el atacante podría hacerse pasar por el BIG-IP ASM Central Policy Builder y enviar datos de sugerencias corruptos o incorrectos al BIG-IQ/Enterprise Manager/F5 iWorkflow. Esto puede dar lugar a sugerencias incorrectas para la elaboración de políticas o a una denegación parcial de servicio (DoS). Se ha reservado el identificador CVE-2019-6665 para esta vulnerabilidad.
- El sistema BIG-IP falla temporalmente al procesar el tráfico cuando se recupera de un reinicio de Traffic Management Microkernel (TMM), y los dispositivos configurados en un grupo de dispositivos pueden fallar. Se han reservado los identificadores CVE-2019-6666 y CVE-2019-6667 para esta vulnerabilidad.
- BIG-IP Edge Client podría permitir que un atacante, sin privilegios en el dispositivo macOS afectado, obtenga la propiedad de los archivos que pertenecen a la cuenta root en el host del cliente local. Se ha reservado el identificador CVE-2019-6668 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad