

— INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

Panorama general y criticidad en las Big Tech durante septiembre. Análisis de inteligencia de seguridad sobre los hallazgos reportados, vulnerabilidades explotables y un análisis a fondo de las amenazas más críticas.

PERIODO

Septiembre 2026

HALLAZGOS

13,548 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

13,548

VULNERABILIDADES DETECTADAS EN SEPTIEMBRE

Una cifra que da cuenta de la amplitud de la superficie de ataque, con más de la mitad de los hallazgos concentrados en las categorías de mayor impacto.

CRÍTICAS

1,506

11.12 % del total

ALTAS

6,275

46.32 % del total

CRÍTICA + ALTA

7,781

57.43 % del total

Septiembre cerró con **13,548 vulnerabilidades con severidad asignada**. La distribución por criticidad muestra **1,506 vulnerabilidades Críticas** (11.12 % del total) y **6,275 de gravedad Alta** (46.32 %). En conjunto, **57.43 %** de los hallazgos del mes corresponde a categorías de riesgo elevado, capaces de derivar en ejecución remota de código, escalada de privilegios o exposición de datos. Las de severidad Media suman 4,836 (35.70 %) y las Bajas 931 (6.87 %).

Esta concentración de riesgos de alto impacto indica que las organizaciones enfrentan una presión considerable para priorizar y remediar un gran volumen de amenazas. El recuento por severidad considera únicamente las categorías Crítica, Alta, Media y Baja; se excluyen del análisis las vulnerabilidades informativas o sin severidad asignada.

El ranking de productos muestra una concentración absoluta en el ecosistema Microsoft. El Top 10 está ocupado **exclusivamente** por versiones de Windows y Windows Server: [windows_server_2025](#) (677) encabeza la lista, seguido de [windows_server_2022](#) (639), [windows_11_26h1](#) y [windows_11_24h2](#) (627 cada uno) y [windows_11_25h2](#) (626). Completan el ranking [windows_server_2019](#) (614), [windows_10_1809](#) (610), [windows_11_23h2](#) (600) y las ramas [windows_10_21h2](#) y [windows_10_22h2](#) (567 cada una). La cercanía de las cifras entre versiones sugiere que buena parte de estas vulnerabilidades afecta transversalmente a todo el parque Windows soportado, desde Windows 10 hasta Windows Server 2025, lo que amplifica su impacto en entornos corporativos.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

Vectores de ataque recurrentes

El examen de las Críticas de septiembre muestra una concentración en el **perímetro y los sistemas de control de acceso**. [Cisco Identity Services Engine](#) acumula al menos cuatro vulnerabilidades críticas en el mes, una de ellas ya explotada. Se suman [SonicWall SMA1000](#), con SSRF previa a la autenticación y explotación confirmada, [HPE Networking Fabric Composer](#), con dos fallos que otorgan acceso administrativo, y los servidores de consola y gateways de gestión [Lantronix SLC](#) y [EMG](#).

En **nube y plataformas gestionadas** destaca Microsoft, con la autenticación como causa dominante: [Azure Active Directory B2C](#), [Microsoft Fabric](#), [Azure Container Registry](#), [Azure AI Language](#), [Azure Billing](#) y [Copilot Studio](#), con suplantación, omisión de autorización, verificación insuficiente de firmas o de autenticidad y funciones críticas sin autenticación.

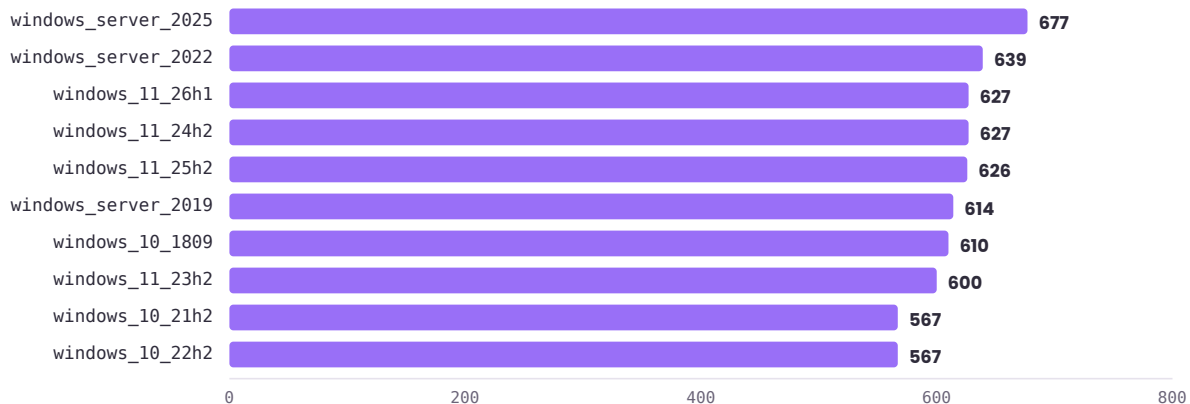
Oracle Fusion Middleware concentra críticas explotables sin autenticación: [Access Manager](#), [Internet Directory](#), [WebLogic Server](#), [Forms](#) y [Platform Security for Java](#).

En **plataformas de IA y agentes**, el foco está en el **Model Context Protocol** (MCP), la capa que conecta asistentes de IA con sistemas corporativos. Al menos tres servidores MCP registran críticas —[MCP Atlassian](#), [MCP Context Forge](#) y [MySQL MCP Server](#)—, junto a [MaxKB](#) y [Google Cloud Agent Development Kit](#). El patrón común es un conector que hereda credenciales o capacidades privilegiadas y las expone a quien logre invocarlo.

En **aplicaciones empresariales** pesa Adobe: al menos ocho Críticas en [Campaign Classic](#), una en [Commerce](#) con explotación confirmada y otra en [Experience Manager Forms JEE](#). Se suman [IBM MQ Appliance](#), [IBM Common Licensing](#), [Apache Storm](#), [Chef Automate](#) y [RTI Connex Professional](#).

El **ecosistema WordPress y Joomla** registra fallos explotables sin autenticación: cargas arbitrarias de archivos en [teddy-bear-customize-addon](#) y [Embed HTML5 Game](#), borrado de archivos u opciones del sitio en [CryptoPayment Gateway](#) y [miniOrange 2FA](#), y en Joomla RCE en [OrdaSoft CCK](#) e inyección SQL en [JCTables](#). En **sistemas operativos**, macOS registra un escape de sandbox por validación insuficiente de entitlements.

Top 10 productos más afectados en septiembre



Número de vulnerabilidades por producto. El Top 10 lo ocupan exclusivamente versiones de Windows y Windows Server.

INTELIGENCIA DE SEGURIDAD • MICROSOFT • GOOGLE • ORACLE

Panorama Big Tech

Este reporte mensual de inteligencia resume las vulnerabilidades identificadas en productos de nuestros principales proveedores tecnológicos durante septiembre.

Microsoft presenta el mayor volumen, con **978 vulnerabilidades**: 53 Críticas, 693 Altas, 231 Medias y 1 Baja. Su perfil está fuertemente sesgado hacia la gravedad Alta: 693 de sus 978 hallazgos (71 %) caen en esa categoría, y solo 53 (5 %) son Críticos. El volumen se concentra en Windows y Windows Server, que ocupan por completo el Top 10 de productos, y se complementa con fallos críticos de autenticación y autorización en servicios de nube.

Google registra **638 vulnerabilidades**: 85 Críticas, 241 Altas, 258 Medias y 54 Bajas. Es el fabricante con el mayor número absoluto de Críticas del grupo (85) y presenta la distribución más equilibrada, con Medias (258) y Altas (241) en proporciones similares. Entre sus Críticas figuran componentes de Android y Android XR.

Oracle reporta **274 vulnerabilidades**: 63 Críticas, 182 Altas, 24 Medias y 5 Bajas. Pese a ser el de menor volumen, presenta el perfil más severo de los tres: 23 % de sus hallazgos son Críticos y 89 % caen en Crítica o Alta. Entre sus Críticas destacan componentes de Fusion Middleware —Access Manager, Internet Directory, WebLogic Server, Forms y Platform Security for Java—, todos explotables de forma remota y sin autenticación.

La lectura conjunta muestra tres perfiles distintos. Microsoft aporta el volumen, concentrado en el sistema operativo y en servicios de nube; Google, el mayor número absoluto de Críticas; y Oracle, la mayor densidad de riesgo por hallazgo, concentrada en su pila de middleware e identidad. Cada perfil exige una respuesta distinta: ventanas de parcheo masivo para el primero y priorización selectiva para los otros dos.

Distribución de severidad por Big Tech



DISTRIBUCIÓN POR FABRICANTE

Severidad por **marca**

Conteo de vulnerabilidades por fabricante y nivel de severidad. La intensidad cromática representa el número de CVE por celda: Microsoft concentra el grueso de los hallazgos de severidad Alta, Google registra el mayor número absoluto de Críticas y Oracle presenta la mayor proporción relativa de hallazgos Críticos del grupo.



MODELO EPSS · PRÓXIMOS 30 DÍAS

Más probables a ser explotadas

Las 10 vulnerabilidades con mayor probabilidad de explotación durante los próximos 30 días, según el modelo EPSS, que estima la probabilidad de que una vulnerabilidad sea usada en un ataque real. Todas presentan una probabilidad cercana al **100 %** y muchas han sido explotadas activamente como días cero.

CVE-2024-7593

EPSS 99.99 %

Ivanti Virtual Traffic Manager (vTM): implementación incorrecta de un algoritmo de autenticación en el panel de administración. Permite a un atacante remoto no autenticado eludir la autenticación y crear una cuenta de administrador a su elección.

EPSS alto: exploit público disponible desde la publicación del aviso y explotación activa confirmada por CISA. Afecta a un controlador de entrega de aplicaciones que se sitúa frente a sitios y aplicaciones expuestos a internet.

CVE-2024-3400

EPSS 99.99 %

Palo Alto Networks GlobalProtect Gateway: inyección de comandos en la interfaz de administración web. Permite a un atacante no autenticado ejecutar comandos arbitrarios con privilegios de root en el dispositivo.

EPSS alto: explotación activa como día cero desde su descubrimiento. Existen exploits públicos y afecta a infraestructuras de red críticas (appliances VPN), facilitando el acceso remoto a entornos protegidos.

CVE-2024-23897

EPSS 99.99 %

Jenkins: lectura de archivos arbitrarios por una falla en la biblioteca `args4j` utilizada por el CLI. Permite a un atacante no autenticado leer cualquier archivo del sistema del controlador de Jenkins.

EPSS alto: exploit público disponible y facilidad de explotación para leer archivos sensibles. Jenkins es una plataforma CI/CD muy extendida y un objetivo de alto valor.

CVE-2024-21893

EPSS 99.99 %

Ivanti Connect Secure y Policy Secure: Server-Side Request Forgery (SSRF) que permite a un atacante autenticado, con privilegios de administrador, realizar peticiones a recursos internos restringidos.

EPSS alto: parte de una cadena de vulnerabilidades activamente explotadas. Aunque requiere autenticación, suele combinarse con otros fallos que permiten el acceso inicial no autenticado a estos sistemas críticos.

CVE-2024-21887

EPSS 99.99 %

Ivanti Connect Secure y Policy Secure: inyección de comandos en los componentes SAML. Permite a un atacante autenticado con privilegios de administrador ejecutar comandos arbitrarios en el dispositivo.

EPSS alto: campaña de explotación en curso contra productos Ivanti. Exploit público disponible y suele encadenarse con otras vulnerabilidades para lograr RCE no autenticada.

CVE-2023-4966

EPSS 99.99 %

Citrix NetScaler ADC y NetScaler Gateway («Citrix Bleed»): divulgación de información que permite a un atacante no autenticado robar tokens de sesión, eludiendo la autenticación.

EPSS alto: explotación activa y generalizada por múltiples grupos de amenazas. Existen exploits públicos y afecta a dispositivos críticos de acceso a red (VPN/ADC).

CVE-2023-44487**EPSS 99.99 %**

«HTTP/2 Rapid Reset Attack»: denegación de servicio que permite abrumar a un servidor enviando un gran número de peticiones HTTP/2 y cancelándolas inmediatamente.

EPSS alto: detalles de explotación y herramientas públicas. Afecta a un protocolo fundamental en numerosos servidores web y proxies, con alta eficacia para ataques DoS contra servicios expuestos a internet.

CVE-2023-35082**EPSS 99.99 %**

Ivanti Endpoint Manager Mobile (EPMM), antes MobileIron Core: omisión de autenticación que permite a un atacante no autenticado acceder a APIs restringidas del sistema.

EPSS alto: explotación activa en la naturaleza y exploits públicos disponibles. Afecta a infraestructuras críticas de gestión de dispositivos móviles (MDM), con alto impacto.

CVE-2023-35078**EPSS 99.99 %**

Ivanti Endpoint Manager Mobile (EPMM), antes MobileIron Core: omisión de autenticación que permite a un atacante no autenticado acceder a APIs específicas utilizadas para la gestión de dispositivos móviles.

EPSS alto: explotación activa y exploits públicos. Similar a CVE-2023-35082, afecta a infraestructuras MDM críticas, habilitando el acceso no autenticado a APIs sensibles del sistema.

CVE-2023-32315**EPSS 99.99 %**

Openfire (servidor de colaboración en tiempo real): path traversal en la interfaz web que permite a un atacante no autenticado subir archivos maliciosos a ubicaciones arbitrarias, lo que puede llevar a RCE.

EPSS alto: explotación activa y exploits públicos. Afecta a un servidor de comunicaciones muy utilizado, permitiendo RCE no autenticada con alto impacto y facilidad de explotación.

! URGENCIA DE PARCHEO, INMEDIATA Y CRÍTICA

Dado que todas estas vulnerabilidades presentan un score EPSS cercano al 100 %, su probabilidad de ser explotadas en los próximos 30 días es máxima. La mayoría están siendo activamente explotadas en la naturaleza, cuentan con exploits públicos y afectan a servicios críticos expuestos a internet —VPN, controladores de entrega de aplicaciones, MDM y CI/CD—. Las organizaciones deben priorizar la aplicación de estos parches sin demora.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-76460

Cisco Identity Services Engine · API

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

Vulnerabilidad en una API de Cisco Identity Services Engine (ISE) que permite a un atacante remoto y no autenticado eludir la autenticación. Afecta también a ISE Passive Identity Connector (ISE-PIC).

1 VECTOR DE ATAQUE

El aviso atribuye el fallo a un control de autenticación insuficiente en un endpoint de la API. Basta con enviar una solicitud manipulada al endpoint afectado para obtener acceso no autorizado al dispositivo, eludiendo la interfaz de administración web. El vector CVSS AV:N/AC:L/PR:N/UI:N/S:C indica explotación remota, de baja complejidad, sin credenciales ni interacción del usuario.

2 IMPACTO TÉCNICO

ISE es el servidor de políticas de control de acceso a la red: decide qué usuarios y dispositivos se conectan, con qué perfil y a qué segmentos. El acceso no autorizado permite alterar políticas de autorización, admitir dispositivos no confiables, desactivar controles de postura o leer datos de identidad. El cambio de alcance refleja que el compromiso afecta a la red que ISE gobierna, no solo al equipo.

3 JUSTIFICACIÓN DEL RIESGO

Es la vulnerabilidad más urgente de esta selección. Fue incorporada al catálogo KEV durante las dos semanas siguientes a su publicación y su EPSS de 14.03 % es el más alto del conjunto crítico analizado. Además, no está sola: en septiembre se publicaron al menos otras tres vulnerabilidades críticas en ISE, entre ellas CVE-2026-76423, que otorga acceso administrativo a través de la API REST. Quien opere ISE debe tratarlo como un activo comprometible desde la red hasta confirmar una versión corregida.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · SSRF PREVIA A LA AUTENTICACIÓN

CVE-2026-83548

SonicWall SMA1000 · Interfaz Work Place
SEVERIDAD Crítica
EXPLOTABLE sin autenticación · remoto

Server-Side Request Forgery previa a la autenticación en la interfaz Work Place del appliance SonicWall SMA1000, originada en una ruta de acceso alternativa no prevista.

1 VECTOR DE ATAQUE

Un atacante remoto no autenticado puede aprovechar esa ruta alternativa para que el appliance emita solicitudes en su nombre y alcanzar funcionalidades sensibles que deberían estar protegidas. El NVD asocia la vulnerabilidad a los modelos SMA 6210, SMA 7210 y SMA 8200v.

2 IMPACTO TÉCNICO

El SMA1000 es el gateway de acceso remoto seguro: la puerta por la que entran usuarios y terceros a la red corporativa. Acceder a sus funciones sensibles permite realizar operaciones no autorizadas sobre el equipo y, desde su posición, alcanzar recursos internos que solo él puede ver. El cambio de alcance (S:C) confirma que el impacto trasciende al appliance.

3 JUSTIFICACIÓN DEL RIESGO

Figura en el catálogo KEV con explotación confirmada y un EPSS de 8.76 %, el segundo más alto del conjunto. Responde al mismo patrón que domina el ranking EPSS de este boletín —Ivanti, Palo Alto, Citrix—: los appliances de acceso remoto expuestos a internet son el objetivo preferente. Publicada el 1 de septiembre, es una prioridad de parcheo inmediata; en equipos que estuvieron expuestos sin parche corresponde además revisar indicadores de compromiso, no solo actualizar.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-75650

Adobe Commerce · Motor de plantillas

SEVERIDAD **Crítica**

EXPLOTABLE **sin interacción del usuario**

Neutralización inadecuada de elementos especiales usados en un motor de plantillas en Adobe Commerce, que puede derivar en ejecución de código arbitrario en el contexto del usuario actual. Afecta también a Adobe Commerce B2B y Magento.

1 VECTOR DE ATAQUE

Se trata de una inyección en el motor de plantillas: una entrada que el atacante controla se interpreta como plantilla y se evalúa en el servidor. El aviso indica que la explotación no requiere interacción del usuario y que el alcance cambia; el vector CVSS (PR:N) indica que tampoco requiere credenciales.

2 IMPACTO TÉCNICO

Ejecución de código en el servidor de la tienda. En una plataforma de comercio electrónico eso alcanza datos de clientes, pedidos y el flujo de pago, donde un atacante puede insertar código para capturar los datos de tarjeta que ingresan los compradores.

3 JUSTIFICACIÓN DEL RIESGO

Figura en el catálogo KEV con explotación confirmada y un EPSS de 3.95 %. Para comercios que procesan pagos con tarjeta, un compromiso del checkout tiene además implicancias de cumplimiento PCI DSS y, al involucrar datos personales de clientes, activa las obligaciones de la Ley 21.719. La remediación debe incluir la revisión de integridad de las plantillas y scripts servidos en el proceso de pago.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-71133

Oracle Access Manager · Motor de Autenticación

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · HTTP**

Vulnerabilidad en el componente Authentication Engine de Oracle Access Manager, dentro de Oracle Fusion Middleware. Afecta a las versiones 12.2.1.4.0 y 14.1.2.1.0 y permite a un atacante no autenticado con acceso de red vía HTTP comprometer el producto.

1 VECTOR DE ATAQUE

El aviso de Oracle la califica como de explotación sencilla, sin autenticación, a través de HTTP, y advierte que los ataques pueden impactar significativamente a productos adicionales por cambio de alcance. El resultado declarado es la toma de control de Oracle Access Manager.

2 IMPACTO TÉCNICO

OAM es la capa de inicio de sesión único y autorización frente a las aplicaciones corporativas. Su toma de control permite eludir la autenticación y la autorización de todo lo que protege, emitir sesiones válidas para cualquier usuario y modificar políticas de acceso.

3 JUSTIFICACIÓN DEL RIESGO

Oracle Access Manager no es el único componente de identidad de Oracle con críticas en septiembre: Oracle Internet Directory (CVE-2026-83059) y Oracle Platform Security for Java (CVE-2026-83020) registran también vulnerabilidades explotables sin autenticación. La concentración de fallos críticos en la pila de identidad de Oracle en un mismo mes indica que no se trata de hallazgos aislados sino de una superficie que requiere un ciclo de parcheo propio.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-83021

Oracle WebLogic Server · Web Container

SEVERIDAD **Crítica**EXPLOTABLE **sin autenticación · HTTP**

Vulnerabilidad en el componente Web Container de Oracle WebLogic Server. Afecta a las versiones 12.2.1.4.0, 14.1.1.0.0 y 14.1.2.0.0 y permite a un atacante no autenticado con acceso de red vía HTTP comprometer el servidor.

1 VECTOR DE ATAQUE

Oracle la califica como de explotación sencilla, sin autenticación y con cambio de alcance. El componente afectado es el contenedor web, la capa que recibe y procesa las solicitudes HTTP antes de entregarlas a las aplicaciones desplegadas, por lo que es alcanzable desde el mismo puerto que atiende a los usuarios.

2 IMPACTO TÉCNICO

Toma de control del servidor de aplicaciones. WebLogic aloja aplicaciones de negocio y es la base de buena parte de Fusion Middleware; su compromiso da acceso a las aplicaciones desplegadas, a sus credenciales de conexión a bases de datos y a los sistemas con que se integran.

3 JUSTIFICACIÓN DEL RIESGO

WebLogic acumula múltiples entradas históricas en el catálogo KEV, lo que lo convierte en un objetivo recurrente tras cada aviso crítico. Aunque a la fecha de cierre esta vulnerabilidad no figura en KEV, el antecedente justifica tratarla con una prioridad equivalente, en especial en servidores alcanzables desde internet.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-83711

Microsoft Azure Active Directory B2C

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

Omisión de autorización mediante una clave controlada por el usuario en Azure Active Directory B2C, que permite a un atacante no autorizado elevar privilegios a través de la red.

1 VECTOR DE ATAQUE

La debilidad descrita corresponde a un patrón en que el servicio decide a qué objeto acceder a partir de un identificador que el solicitante puede modificar, sin comprobar que tenga derecho sobre él. El vector AV:N/AC:L/PR:N/UI:N/S:C indica un ataque remoto, de baja complejidad y sin credenciales, con impacto alto en confidencialidad e integridad. Microsoft no ha publicado el detalle del mecanismo afectado.

2 IMPACTO TÉCNICO

Azure AD B2C es el servicio de identidad para clientes externos: gestiona el registro, el inicio de sesión y los perfiles de los usuarios de aplicaciones de cara al público. Elevar privilegios en ese plano puede permitir acceder a cuentas de clientes o modificar sus atributos de identidad.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica para organizaciones que usan B2C en canales digitales —banca en línea, portales de seguros, aplicaciones de salud—, donde la base de usuarios son personas naturales y un acceso indebido a sus perfiles activa las obligaciones de la Ley 21.719. Forma parte de un conjunto más amplio: en septiembre se publicaron críticas de autenticación o autorización en Microsoft Fabric, Azure Container Registry, Azure AI Language, Azure Billing y Copilot Studio.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-82004

Adobe Campaign Classic

SEVERIDAD **Crítica**

EXPLOTABLE **sin interacción del usuario**

Neutralización inadecuada de elementos especiales usados en un comando del sistema operativo (inyección de comandos SO) en Adobe Campaign Classic, que puede derivar en ejecución de código arbitrario en el contexto del usuario actual.

1 VECTOR DE ATAQUE

El aviso indica que la explotación no requiere interacción del usuario y que el alcance cambia. La inyección de comandos SO implica que una entrada controlable por el atacante alcanza un intérprete de comandos del sistema sin saneamiento suficiente.

2 IMPACTO TÉCNICO

Ejecución de código en el servidor de campañas. Campaign Classic concentra bases de datos de clientes, segmentaciones y la infraestructura de envío masivo de correo, lo que habilita tanto la exfiltración de datos personales como el uso de la plataforma legítima de la organización para campañas de phishing.

3 JUSTIFICACIÓN DEL RIESGO

Con un EPSS de 3.25 % es una de las críticas con mayor probabilidad estimada del conjunto analizado, y es solo una de ocho vulnerabilidades críticas de Campaign Classic en el conjunto analizado —inyección de código, autorización incorrecta y SSRF—. La acumulación de fallos críticos en un mismo producto durante un solo mes obliga a verificar que la plataforma reciba la atención de parcheo que su exposición exige.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · SUPLANTACIÓN DE IDENTIDAD

CVE-2026-77244

MCP Atlassian · Transporte HTTP

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · red**

En versiones anteriores a la 0.22.0, el servidor MCP Atlassian —que conecta asistentes de IA con Confluence y Jira mediante el Model Context Protocol— acepta solicitudes por su transporte HTTP sin una identidad de usuario verificada.

1 VECTOR DE ATAQUE

Cuando no hay una identidad verificada, la construcción del cliente hacia Atlassian recurre a las credenciales globales de Jira o Confluence configuradas por el operador. Cualquier cliente de red que alcance el endpoint MCP puede invocar las herramientas de Atlassian como si fuera el operador. El aviso traza el flujo vulnerable a través de `UserTokenMiddleware`, `AtlassianOpaqueTokenVerifier`, `_get_fetcher` y el transporte `streamable-http`.

2 IMPACTO TÉCNICO

El atacante obtiene las operaciones de lectura y escritura disponibles para la cuenta del operador en Confluence y Jira: documentación interna, incidencias y procedimientos operativos. El impacto en confidencialidad e integridad es alto. Corregido en 0.22.0.

3 JUSTIFICACIÓN DEL RIESGO

El fallo ilustra el riesgo central de los conectores de IA: se despliegan con una cuenta de servicio privilegiada y heredan sus permisos hacia quien logre hablarles. En septiembre registran críticas al menos otros dos servidores MCP —MCP Context Forge, con un escape de sandbox que llega a ejecutar comandos del sistema, y MySQL MCP Server—. Los servidores MCP deben inventariarse y tratarse como identidades privilegiadas, no como utilidades de desarrollo.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-80155

Lantronix SLC y EMG · Portal de gestión web
SEVERIDAD Crítica
EXPLOTABLE sin autenticación

Bypass de autenticación en el endpoint de carga del portal de gestión web de los servidores de consola y gateways de gestión Lantronix SLC8000 (firmware anterior a v9.7.0.5), SLC9000 (anterior a v9.7.0.2), EMG8500 y EMG7500 (anterior a v9.7.0.1), y en todas las versiones de SLB882, SLCx-03 y SLCx-02.

1 VECTOR DE ATAQUE

Según el aviso, el servidor de configuración construye la ruta del archivo de cookie de sesión con un búfer de tamaño fijo. Una cookie de longitud específica trunca esa ruta y, combinada con path traversal, redirige la validación de sesión hacia un archivo arbitrario del disco, eludiendo las comprobaciones. Desde ahí el atacante puede leer configuración sensible y subir archivos a ubicaciones arbitrarias, hasta lograr ejecución remota de código.

2 IMPACTO TÉCNICO

Pérdida total de confidencialidad, integridad y disponibilidad del equipo y, según el aviso, posible impacto en los dispositivos conectados por puerto serie. Un servidor de consola da acceso fuera de banda a la consola de routers, firewalls, switches y servidores: es la vía de administración que se usa cuando todo lo demás falla.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por la posición del equipo: quien controla el servidor de consola controla la infraestructura que administra, por debajo de los controles de red. Para operadores de infraestructura crítica sujetos a la Ley 21.663, la red de gestión fuera de banda debe estar aislada y su exposición verificada. Que tres modelos estén afectados en todas sus versiones obliga a mitigar por segmentación donde no exista firmware corregido.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-10747

IBM MQ Appliance
SEVERIDAD Crítica
EXPLOTABLE sin autenticación · remoto

Desbordamiento de búfer en el heap durante el procesamiento de mensajes de protocolo, antes de la autenticación, en IBM MQ Appliance. Puede causar denegación de servicio o, potencialmente, ejecución de código arbitrario.

1 VECTOR DE ATAQUE

El fallo se produce al procesar mensajes del protocolo antes de que exista autenticación, por lo que basta con alcanzar el puerto de escucha del appliance. Un mensaje malformado corrompe memoria del heap. El vector CVSS AV:N/AC:L/PR:N/UI:N/S:C confirma un ataque remoto, de baja complejidad y sin credenciales.

2 IMPACTO TÉCNICO

En el escenario de menor impacto, la caída del gestor de colas; en el peor, ejecución de código en el appliance. MQ transporta mensajes entre sistemas de negocio —transacciones, órdenes, notificaciones—, de modo que su interrupción detiene la integración y su compromiso permite leer o alterar mensajes en tránsito.

3 JUSTIFICACIÓN DEL RIESGO

Es especialmente relevante para banca y seguros, donde IBM MQ es habitual como columna de integración entre el core, los canales y los sistemas de pago. Un fallo previo a la autenticación en esa capa combina impacto sobre la disponibilidad, con implicancias de continuidad operacional para entidades supervisadas por la CMF, y sobre la integridad de las transacciones. Corresponde verificar que los puertos de MQ no sean alcanzables desde segmentos no confiables.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

Septiembre cerró con **13,548 vulnerabilidades** y un 57.43 % concentrado en las categorías Crítica y Alta. Tres rasgos definen el mes: Microsoft aporta el mayor volumen y ocupa por completo el Top 10 de productos, la explotación confirmada recae sobre equipos de perímetro y de control de acceso, y los conectores de IA basados en MCP aparecen como una superficie con fallos de identidad.

01 Parchear primero el perímetro con explotación confirmada

26 vulnerabilidades publicadas en septiembre ya figuran en el catálogo KEV, y CISA incorporó 43 entradas durante el mes. Tres de las Críticas analizadas —Cisco ISE, SonicWall SMA1000 y Adobe Commerce— fueron explotadas a pocas semanas de su publicación, y las tres son sistemas alcanzables desde internet o que gobiernan el acceso a la red. La cola de remediación debe ordenarse por explotación confirmada y exposición, con los equipos de acceso remoto y de control de acceso a la red al frente.

02 Gobernar los conectores de IA como identidades privilegiadas

Los servidores MCP conectan asistentes de IA con Jira, Confluence, bases de datos y otros sistemas usando cuentas de servicio con permisos amplios. El caso de MCP Atlassian muestra que, si el conector no verifica la identidad de quien lo invoca, entrega esos permisos a cualquiera que lo alcance. Se requiere inventario de los servidores MCP desplegados, autenticación obligatoria en sus transportes de red, credenciales por usuario en lugar de cuentas compartidas y restricción de las herramientas que ejecutan código.

03 Sostener un ciclo de parcheo propio para la pila de identidad

Oracle Access Manager, Oracle Internet Directory y Oracle Platform Security for Java registran Críticas explotables sin autenticación en el mismo mes, y Microsoft suma fallos de autenticación en Azure AD B2C y en otros cinco servicios de nube. Esta acumulación indica que la identidad corporativa y de clientes no puede esperar al ciclo general de parcheo: requiere inventario de los proveedores de identidad en uso, reducción de su exposición de red y un procedimiento de respuesta específico ante su compromiso.



Identifica y prioriza las vulnerabilidades de tu organización, **antes que lo haga un atacante.**

BOLETÍN DE VULNERABILIDADES · SEPTIEMBRE 2026