BASELINE

INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

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

PERIODO
Octubre 2026

HALLAZGOS
15,525 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

15,525

VULNERABILIDADES DETECTADAS EN OCTUBRE

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	ALTAS	CRÍTICA + ALTA
1,543	6,646	8,189
9.94 % del total	42.81 % del total	52.75 % del total

Octubre cerró con **15,525 vulnerabilidades con severidad asignada**. La distribución por criticidad muestra **1,543 vulnerabilidades Críticas** (9.94 % del total) y **6,646 de gravedad Alta** (42.81 %). En conjunto, **52.75 %** 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 6,366 (41.00 %) y las Bajas 970 (6.25 %).

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` (1,030) encabeza la lista, seguido de `windows_11_24h2` y `windows_11_25h2` (1,001 cada uno), `windows_11_26h1` (993) y `windows_11_26h2` (989). Completan el ranking `windows_server_2022` (966), `windows_11_23h2` (957), `windows_server_2019` (902) y las ramas `windows_10_21h2` y `windows_10_22h2` (890 cada una). La cercanía de las cifras entre versiones confirma que buena parte de estas vulnerabilidades afecta transversalmente a todo el parque Windows soportado, desde Windows 10 hasta Windows Server 2025, con más de mil vulnerabilidades asociadas a una sola versión.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

Vectores de ataque recurrentes

El hecho más relevante del mes es la divulgación de dos vulnerabilidades críticas en el **núcleo de PHP** (CVE-2026-109618 y CVE-2026-109619, conocidas como **PHP2Shell**), que permiten ejecución remota de código sin autenticación y encabezan el ranking EPSS de este boletín. Dada su importancia, se analizan en una sección propia más adelante.

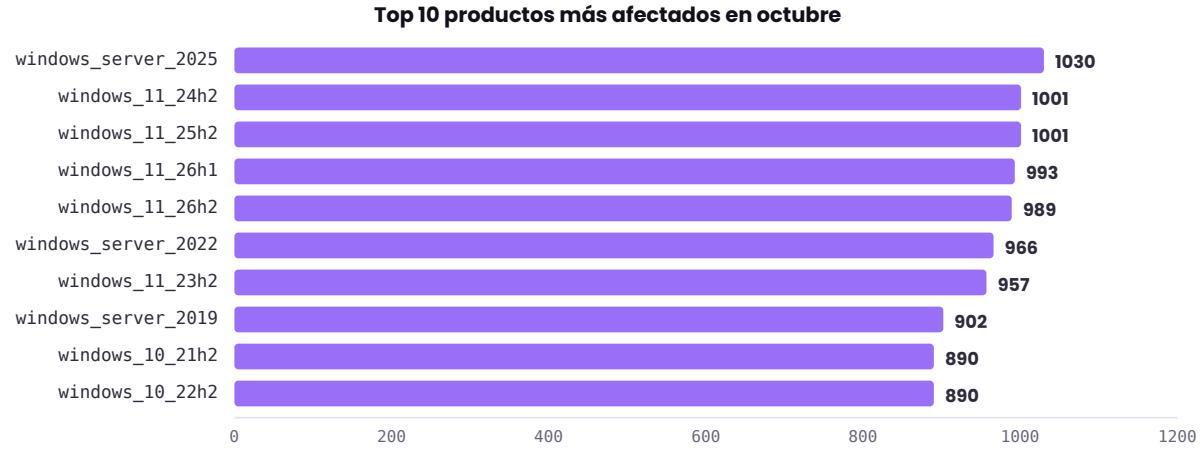
El vector dominante entre las Críticas es la **ejecución remota de código sin autenticación**, presente en appliances de red, plataformas de desarrollo y gestores de contenido. En **infraestructura de red** destacan múltiples fallos en HPE Aruba AOS-8 y AOS-10 —desbordamientos de búfer, inyección de comandos e inyección SQL—, todos explotables sin autenticación.

En **plataformas de desarrollo y DevOps** se concentra un grupo relevante: GitLab CE/EE con RCE por desbordamiento de enteros, JetBrains TeamCity con escape del sandbox de Kotlin DSL, Perforce P4 Search con un token por defecto y Apache Camel con deserialización no confiable.

El **ecosistema de gestores de contenido** acumula RCE no autenticadas en Adobe Commerce y Magento, la familia ColdFusion (carga de archivos, SSRF e inyección de código), Adobe Experience Manager, Adobe Campaign Classic y el complemento YOOtheme Pro para Joomla.

En **nube y plataformas gestionadas** reaparecen fallos de autenticación y autorización en servicios de Microsoft: Azure Kubernetes Configuration Service, VM Inspector para Azure y Azure Virtual Machines, en general por funciones críticas sin autenticación o resolución insegura de enlaces.

Una tendencia persistente son las **plataformas de IA y agentes** con autenticación ausente: NVIDIA NeMo Agent Toolkit, NVIDIA AIStore y Loom for AWS, esta última con toma de control del plano de control de agentes. El **respaldo y almacenamiento** es otro flanco: Ahsay Cloud Backup Suite, con inyección de comandos ya explotada, y Dell Container Storage Modules.



Número de vulnerabilidades por producto. El Top 10 lo ocupan exclusivamente versiones de Windows y Windows Server, con más de mil vulnerabilidades en la versión más afectada.

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 octubre.

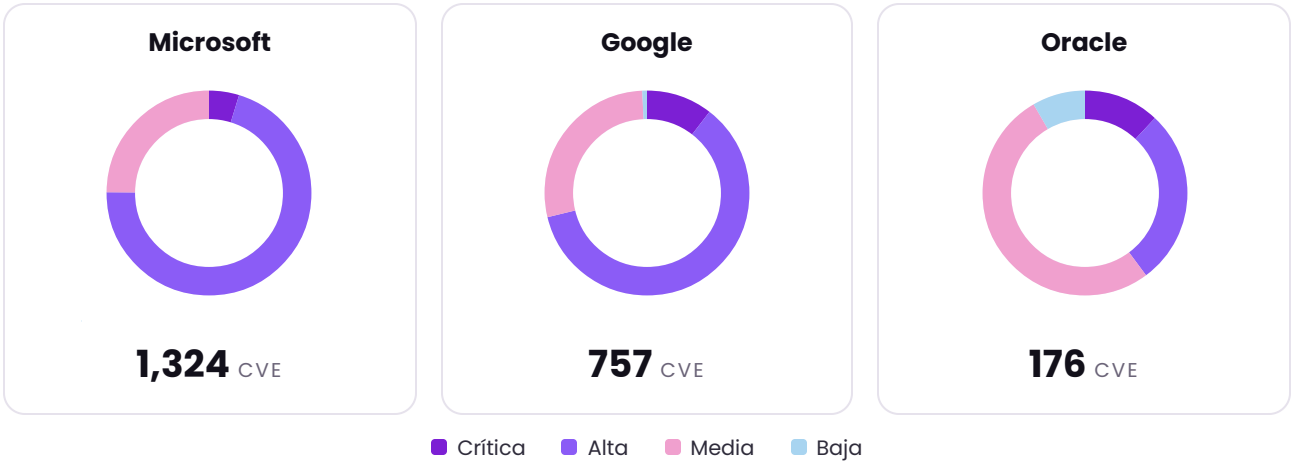
Microsoft presenta el mayor volumen, con **1,324 vulnerabilidades**: 63 Críticas, 930 Altas, 331 Medias y 0 Bajas. Su perfil está fuertemente sesgado hacia la gravedad Alta: 930 de sus 1,324 hallazgos (70 %) caen en esa categoría, y 63 (5 %) son Críticos. El volumen se concentra en Windows y Windows Server, que ocupan por completo el Top 10 de productos, y se complementa con fallos críticos de autenticación en servicios de nube.

Google registra **757 vulnerabilidades**: 79 Críticas, 459 Altas, 212 Medias y 7 Bajas. Es el segundo en volumen y presenta un número alto de hallazgos de gravedad Alta (459), concentrados predominantemente en el navegador Chrome y en el sistema operativo Android.

Oracle reporta **176 vulnerabilidades**: 21 Críticas, 49 Altas, 91 Medias y 15 Bajas. Es el de menor volumen de los tres, con una distribución inusualmente cargada hacia la severidad Media (91). Entre sus Críticas destaca un fallo en el componente Workflow de Oracle E-Business Suite, explotable de forma remota y sin autenticación, con toma de control del producto.

La lectura conjunta muestra tres perfiles distintos. Microsoft aporta el grueso del volumen, concentrado en el sistema operativo y en servicios de nube; Google, un volumen alto de severidad Alta en navegador y móvil; y Oracle, un número acotado de hallazgos pero con críticas de alto impacto en sus aplicaciones de negocio. 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 aporta el segundo mayor volumen de Altas y Oracle presenta una distribución cargada hacia la severidad Media.

MICROSOFT
1,324
63 crít · 930 altas

GOOGLE
757
79 crít · 459 altas

ORACLE
176
21 crít · 49 altas

Mapa de calor por marca y severidad



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. Este mes, las dos primeras posiciones las ocupan las vulnerabilidades de PHP divulgadas en octubre.

CVE-2026-109619

EPSS 99.99 %

PHP (núcleo del lenguaje): ejecución remota de código por corrupción de estado interno tras un error fatal. Un atacante no autenticado puede lograr la ejecución de código en el servidor. Forma parte de PHP2Shell.

EPSS alto: EPSS en el máximo (99.99 %), figura en el catálogo KEV y hay explotación activa confirmada en la naturaleza. PHP sostiene una fracción enorme de los sitios de internet. Se analiza en detalle en la sección siguiente.

CVE-2026-109618

EPSS 99.99 %

PHP (núcleo del lenguaje): ejecución remota de código por corrupción de memoria durante el manejo de condiciones de falta de memoria (out-of-memory). Explotable sin autenticación. La segunda mitad de PHP2Shell.

EPSS alto: EPSS en el máximo (99.99 %) y presencia en KEV. Fue la primera de las dos confirmada con ejecución de código en entornos reales. Afecta a PHP 5.4 y posteriores, un universo de despliegues enorme.

CVE-2025-53770

EPSS 99.99 %

Microsoft SharePoint Server (on-premises): ejecución remota de código no autenticada por deserialización insegura en el componente ToolPane, conocida como «ToolShell».

EPSS alto: explotación activa y generalizada desde su divulgación, con despliegue de web shells y robo de claves criptográficas del servidor. Afecta a SharePoint 2016, 2019 y Subscription Edition expuestos a internet.

CVE-2024-7593

EPSS 99.99 %

Ivanti Virtual Traffic Manager (vTM): implementación incorrecta del algoritmo de autenticación del panel de administración, que permite a un atacante remoto crear una cuenta de administrador.

EPSS alto: exploit público disponible 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.

! 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 —el intérprete PHP, servidores de colaboración, controladores de entrega de aplicaciones, VPN y CI/CD—. Las organizaciones deben priorizar la aplicación de estos parches sin demora.

DESTACADO DEL MES · AMENAZA DE ALTO IMPACTO

PHP2Shell: CVE-2026-109618 y CVE-2026-109619

Dos vulnerabilidades críticas en el núcleo de PHP, divulgadas el 21 de octubre de 2026, que permiten ejecución remota de código sin autenticación. PHP sostiene cerca del 70 % de los sitios web, de modo que su superficie de exposición es una de las mayores registradas en el año. Ambas ocupan el primer lugar del ranking EPSS de este boletín, con probabilidad en el máximo.

CVE-2026-109618

RCE · OOM

Corrupción de memoria durante el manejo de condiciones de falta de memoria (out-of-memory). PHP puede quedar interrumpido mientras datos internos de una petición están solo parcialmente inicializados, y la rutina de limpieza posterior trata esa memoria inválida como válida, lo que deriva en ejecución de código.

Vector: RCE no autenticada, CVSS v4.0 9.2. Fue la primera de las dos confirmada con ejecución de código contra un entorno real.

CVE-2026-109619

RCE · estado

Estado interno propiedad de una petición que sobrevive después de que su memoria de respaldo ha sido liberada. Una petición posterior atendida por el mismo worker puede usar ese estado obsoleto antes de que la inicialización normal lo reinicie, permitiendo la ejecución de código.

Vector: RCE no autenticada, CVSS v4.0 9.2. Encabeza el ranking EPSS con probabilidad en el máximo.

1 ALCANCE Y VERSIONES AFECTADAS

El PHP Security Team publicó parches de emergencia el 21 de octubre de 2026 en las versiones 8.5.12, 8.4.27, 8.3.36 y 8.2.35. Están afectadas las versiones desde PHP 5.4 hasta 8.5.11, es decir, prácticamente todo el parque desplegado. Las ramas 8.1, 8.0, 7.x y 5.x están al final de su vida y no reciben parches oficiales, por lo que requieren actualizar a una versión soportada. El equipo de PHP proporcionó además backports de código fuente para quienes compilan desde fuente.

2 EXPLOTACIÓN Y RESPUESTA DE CISA

CISA incorporó ambas vulnerabilidades a su catálogo KEV el 26 de octubre de 2026, confirmando explotación activa, y bajo la directiva BOD 26-04 fijó para las agencias federales un plazo de remediación al 29 de octubre. Investigadores de seguridad detectaron intentos de explotación incluso antes de la publicación de los parches, y laboratorios de inteligencia de amenazas registraron decenas de miles de peticiones de explotación desde centenares de direcciones IP en todo el mundo. La tasa de parcheo global reportada en los primeros días fue baja.

3 RECOMENDACIONES DE REMEDIACIÓN

Primero, inventariar todos los despliegues de PHP del entorno, incluidos los embebidos en appliances y contenedores, priorizando los sistemas expuestos a internet. Segundo, actualizar a una versión parcheada (8.2.35, 8.3.36, 8.4.27 u 8.5.12 o superiores). Donde no sea posible parchear de inmediato, deshabilitar `session.upload_progress` reduce la exposición al vector conocido, y una regla de WAF ofrece protección temporal. Por la existencia de explotación previa a la divulgación, en sistemas que estuvieron expuestos sin parche corresponde asumir compromiso y realizar búsqueda de indicadores, no solo actualizar.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · INYECCIÓN DE COMANDOS

CVE-2026-105134

Ahsay Cloud Backup Suite · Replication Receiver

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Inyección de comandos del sistema operativo en el componente Replication Receiver de Ahsay Cloud Backup Suite (AhsayCBS), en el endpoint `/rps/api/json/UpdateReceivers.do`. Afecta a las versiones hasta 9.15.2.69 y 10.3.4.44.

1 VECTOR DE ATAQUE

La manipulación del argumento `random` permite inyectar comandos del sistema operativo. El ataque se realiza de forma remota y existe exploit público. El aviso advierte además que el primer parche no corrigió adecuadamente el fallo, lo que obligó a actualizar la entrada del CVE: solo las versiones 9.15.2.70 y 10.3.4.45 resuelven el problema.

2 IMPACTO TÉCNICO

Ejecución de comandos arbitrarios en el servidor de respaldo. Una plataforma de backup centraliza copias de múltiples sistemas y suele operar con privilegios amplios sobre la red; su compromiso da acceso a los datos respaldados y puede usarse para desactivar o manipular las copias, un paso habitual en campañas de ransomware.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima urgencia: tiene EPSS de 81.76 %, figura en el catálogo KEV con explotación confirmada y cuenta con exploit público. El hecho de que el parche inicial fuera insuficiente agrava el riesgo, porque instalaciones que se creían corregidas siguen expuestas. La verificación de la versión exacta es imprescindible.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-103849

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, con posible elevación de acceso sobre la cuenta o la sesión de la víctima.

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 de Adobe indica que la explotación no requiere interacción del usuario y que el alcance cambia (S:C).

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

Para comercios que procesan pagos con tarjeta, un compromiso del proceso de pago tiene implicancias de cumplimiento PCI DSS y, al involucrar datos personales de clientes, activa las obligaciones de la Ley 21.719. Adobe Commerce acumula además otras Críticas en el mes en la familia ColdFusion y Experience Manager; la remediación debe incluir la revisión de integridad de las plantillas servidas en el checkout.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-101809

Oracle E-Business Suite · Workflow Notification Mailer

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · HTTP**

> Vulnerabilidad en el componente Workflow Notification Mailer del producto Workflow de Oracle E-Business Suite. Afecta a las versiones 12.2.3 a 12.2.15 y permite a un atacante no autenticado con acceso de red vía HTTP comprometer Workflow.

1 VECTOR DE ATAQUE

El propio aviso de Oracle la califica como de explotación sencilla, sin autenticación, a través de HTTP, con vector CVSS 3.1 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). El resultado declarado es la toma de control de Workflow, y Oracle advierte que los ataques pueden impactar significativamente a productos adicionales por cambio de alcance.

2 IMPACTO TÉCNICO

Oracle E-Business Suite es la columna de procesos de negocio —finanzas, compras, recursos humanos— en muchas organizaciones grandes. El componente de notificaciones de Workflow procesa correo, lo que lo hace alcanzable, y su compromiso da un punto de entrada hacia datos y procesos críticos del ERP.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad por el tipo de sistema que afecta. Oracle E-Business Suite ha sido blanco de campañas de explotación masiva dirigidas a su componente de Workflow, por lo que un fallo no autenticado de puntuación 10.0 en esa superficie debe tratarse como prioridad de parcheo inmediata en toda organización que opere el ERP.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-110264

GitLab CE/EE

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Ejecución remota de código en GitLab Community y Enterprise Edition por un desbordamiento de enteros al compilar una expresión regular especialmente diseñada. Bajo determinadas condiciones, permite a un usuario no autenticado ejecutar código en el servidor.

1 VECTOR DE ATAQUE

El fallo se origina en el manejo de una expresión regular manipulada que provoca un desbordamiento de enteros durante su compilación. Afecta a un amplio rango de versiones, desde la 7.0 hasta las ramas 19.x previas a las correcciones de octubre.

2 IMPACTO TÉCNICO

GitLab aloja el código fuente, las canalizaciones de CI/CD y, con frecuencia, credenciales y secretos de despliegue. La ejecución de código en el servidor permite acceder a repositorios privados, alterar canalizaciones para inyectar código en los artefactos construidos y pivotar hacia los entornos a los que GitLab tiene acceso.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por su posición en la cadena de suministro de software: comprometer GitLab permite insertar código malicioso en productos legítimos antes de su despliegue. El amplísimo rango de versiones afectadas implica que muchas instalaciones de larga data están expuestas. Dado que el servidor suele ser accesible para toda la organización, la actualización no debe postergarse.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-78162

Apache Camel · componente camel-hazelcast

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Deserialización de datos no confiables en Apache Camel. El componente camel-hazelcast crea, en dos de sus rutas de configuración, instancias de Hazelcast cuya deserialización Java no tiene restricciones. Afecta a las versiones 4.0.0 a 4.18.5 y 4.19.0 a 4.22.1.

1 VECTOR DE ATAQUE

Una corrección previa (CVE-2026-43865) añadió un filtro de serialización, pero no alcanzó a dos rutas que Camel construye por sí mismo. Un atacante capaz de publicar en el clúster Hazelcast al que la instancia está conectada puede provocar que un objeto Java de su elección se deserialice dentro de la capa de serialización de Hazelcast, antes de que Camel procese el intercambio, logrando ejecución de código. Los clústeres Hazelcast no tienen autenticación ni TLS habilitados por defecto.

2 IMPACTO TÉCNICO

Ejecución de código en el proceso que integra los sistemas. Apache Camel es un motor de integración que conecta aplicaciones y servicios heterogéneos, de modo que su compromiso da acceso a los flujos de datos que transitan entre ellos y a los sistemas conectados.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por la combinación de deserialización no restringida y la ausencia de autenticación por defecto en Hazelcast: la elección del modo cliente es una decisión de topología, no de seguridad, por lo que ninguna de las rutas vulnerables exige que el despliegue opte explícitamente por una configuración insegura. Corregido en 4.23.0, 4.22.1 y 4.18.5.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-106218

JetBrains TeamCity

SEVERIDAD **Crítica**

EXPLOTABLE **escape de sandbox**

> Escape del sandbox de Kotlin DSL en JetBrains TeamCity que conduce a ejecución remota de código en el servidor. Afecta a las versiones anteriores a 2026.1.3 y 2025.11.7.

1 VECTOR DE ATAQUE

TeamCity permite definir la configuración de compilación mediante un DSL basado en Kotlin, que debería ejecutarse en un entorno restringido. El fallo permite escapar de ese sandbox y ejecutar código arbitrario en el servidor que procesa la definición.

2 IMPACTO TÉCNICO

El servidor de integración continua tiene acceso al código fuente, a las credenciales de despliegue y a los agentes de compilación. La ejecución de código en TeamCity permite robar secretos, manipular los artefactos producidos e inyectar código en la cadena de construcción.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y se suma a GitLab y Perforce entre las plataformas de desarrollo con RCE este mes, lo que confirma la cadena de suministro de software como superficie prioritaria. TeamCity ha sido objetivo de campañas de explotación tras avisos anteriores, por lo que la actualización a 2026.1.3 o 2025.11.7 debe aplicarse con prontitud.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-112816

Canonical LXD · Listener HTTPS

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Validación incorrecta de certificados en el listener HTTPS de Canonical LXD que permite a un atacante no autenticado autenticarse como cualquier cliente de confianza y obtener acceso completo al clúster y a las máquinas virtuales gestionadas, mediante una cadena de certificados manipulada.

1 VECTOR DE ATAQUE

LXD autentica a los clientes por certificado. El fallo en la validación de la cadena permite que un certificado manipulado sea aceptado como el de un cliente de confianza, eludiendo por completo el control de acceso. Afecta a las ramas 4.0, 5.0, 5.21 y 6.9 previas a las versiones corregidas.

2 IMPACTO TÉCNICO

Acceso total al clúster LXD y a las máquinas virtuales y contenedores que gestiona. Equivale a obtener el control del hipervisor: el atacante puede crear, modificar o eliminar instancias, acceder a su contenido y usar la plataforma como punto de pivote.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica porque el compromiso no es de una carga de trabajo sino de la capa de virtualización que las aloja a todas. En entornos que usan LXD para consolidar sistemas, un atacante no autenticado con una cadena de certificados manipulada obtiene control sobre toda la infraestructura virtualizada.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-79851

HPE Aruba Networking · AOS-10

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Desbordamientos de búfer en la interfaz afectada de HPE Aruba Networking AOS-10 que pueden conducir a ejecución remota de código no autenticada, enviando paquetes especialmente diseñados a la interfaz.

1 VECTOR DE ATAQUE

El envío de paquetes manipulados a la interfaz afectada desborda un búfer y permite la ejecución de código arbitrario como usuario privilegiado en el sistema operativo subyacente. Forma parte de un conjunto de fallos divulgados en el mes que afecta tanto a AOS-10 como a AOS-8, con vectores de desbordamiento, inyección de comandos e inyección SQL.

2 IMPACTO TÉCNICO

Compromiso completo del sistema. AOS es el sistema operativo de la infraestructura inalámbrica y de red de HPE Aruba; el control del controlador permite interceptar o redirigir tráfico, acceder a segmentos internos y usar el equipo como punto de apoyo dentro de la red.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por tratarse de infraestructura de red no autenticada, alcanzable desde la red y con ejecución de código como usuario privilegiado. Para operadores de infraestructura crítica sujetos a la Ley 21.663, un controlador de red comprometible sin credenciales es un hallazgo de exposición que debe cerrarse con prontitud, verificando además que la interfaz de gestión no sea alcanzable desde segmentos no confiables.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-103956

Loom for AWS · Plano de control de agentes

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Falta de autenticación para una función crítica en la dependencia de autenticación de Loom for AWS, en versiones anteriores a 1.6.1. En despliegues sin un proveedor de identidad configurado, permite a actores remotos obtener autoridad de superadministrador sobre el plano de control de agentes.

1 VECTOR DE ATAQUE

Cuando no hay proveedor de identidad configurado, cualquier petición a la API de la aplicación obtiene privilegios de superadministrador. Desde ahí el atacante puede registrar servidores de herramientas, leer credenciales de integración almacenadas y reescribir las políticas de rol de IAM asociadas a los roles de agente gestionados.

2 IMPACTO TÉCNICO

Control total del plano de control de agentes de IA en AWS. La capacidad de reescribir políticas de IAM y leer credenciales de integración permite escalar desde la plataforma de agentes hacia la cuenta de AWS subyacente y los servicios que esta gobierna.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y representa el patrón de riesgo de la infraestructura de agentes de IA: plataformas que se despliegan con autenticación opcional y que, sin un proveedor de identidad, quedan completamente abiertas. Se suma a NVIDIA NeMo Agent Toolkit y NVIDIA AIStore entre los fallos de autenticación ausente en plataformas de IA del mes. Corresponde verificar que todo despliegue de agentes tenga autenticación forzada.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · CREDENCIAL POR DEFECTO

CVE-2026-100103

Perforce P4 Search

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Las imágenes de contenedor de Perforce P4 Search anteriores a la versión 2026.4.2 restablecen el token de autenticación del servicio a un valor por defecto públicamente documentado. Un atacante no autenticado con acceso de red puede obtener el máximo privilegio de la aplicación.

1 VECTOR DE ATAQUE

El token de servicio queda fijado a un valor conocido y publicado en la documentación. Cualquier atacante que alcance el servicio por red puede usar ese token para autenticarse con el privilegio más alto, sin necesidad de credenciales propias.

2 IMPACTO TÉCNICO

Control total de la aplicación de búsqueda y, a través de ella, posible ejecución de código y compromiso del servidor P4 conectado. Perforce gestiona el control de versiones en entornos de desarrollo, en particular en sectores como videojuegos y manufactura, por lo que su compromiso alcanza el código y los activos versionados.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por la facilidad de explotación: no hay que vulnerar nada, basta con conocer un token que está en la documentación pública. Es otro eslabón de la cadena de suministro de software comprometida en el mes, junto con GitLab, TeamCity y Apache Camel. La actualización a 2026.4.2 o superior es la única corrección.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

Octubre cerró con **15,525 vulnerabilidades** y un 52.75 % concentrado en las categorías Crítica y Alta. Tres rasgos definen el mes: la divulgación de PHP2Shell en el núcleo de PHP, con explotación confirmada y una superficie de exposición enorme; la concentración de RCE no autenticadas en la cadena de suministro de software; y la persistencia de fallos de autenticación ausente en plataformas de IA y de respaldo.

01 Atender PHP2Shell como una emergencia transversal

Las dos vulnerabilidades de PHP afectan a prácticamente todo el parque desplegado del lenguaje, tienen explotación confirmada y encabezan el ranking EPSS. La exposición no se limita a aplicaciones web propias: PHP está embebido en appliances, contenedores y productos de terceros. Se requiere un inventario completo de despliegues de PHP, actualización inmediata a una versión parcheada y, en sistemas que estuvieron expuestos, búsqueda de indicadores de compromiso, dado que hubo explotación previa a la publicación de los parches.

02 Blindar la cadena de suministro de software

GitLab, JetBrains TeamCity, Perforce P4 Search y Apache Camel concentran ejecución remota de código en las plataformas que compilan y distribuyen software. Comprometer cualquiera de ellas permite inyectar código malicioso en productos legítimos antes de su despliegue. Se requiere tratar los servidores de desarrollo e integración como activos de alto valor: reducir su exposición de red, aplicar sus parches con prioridad y auditar las credenciales y secretos que custodian.

03 Forzar autenticación en plataformas de IA, respaldo y virtualización

Loom for AWS, NVIDIA NeMo Agent Toolkit, Ahsay Cloud Backup Suite y Canonical LXD comparten un mismo patrón: funciones críticas accesibles sin autenticación o con credenciales por defecto, en plataformas que gobiernan agentes, copias de respaldo o máquinas virtuales completas. Corresponde inventariar estas plataformas, exigir autenticación obligatoria, eliminar credenciales por defecto y verificar que ninguna quede expuesta a la red sin control de acceso.

BASELINE

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

BOLETÍN DE VULNERABILIDADES · OCTUBRE 2026