BASELINE

INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

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

PERIODO
Agosto 2026

HALLAZGOS
11,567 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

11,567

VULNERABILIDADES DETECTADAS EN AGOSTO

Un volumen 16.6 % superior al de julio, con un desplazamiento marcado hacia las categorías de mayor impacto y un cambio de composición respecto del mes anterior.

CRÍTICAS	ALTAS	CRÍTICA + ALTA
1,818	**5,270**	**7,088**
15.72 % del total	45.56 % del total	61.28 % del total

Agosto cerró con **11,567 vulnerabilidades con severidad asignada**, frente a las 9,919 de julio. El aumento no fue solo de volumen: las **Críticas pasaron de 1,307 a 1,818** (+39.1 %) y las de gravedad **Alta de 4,114 a 5,270** (+28.1 %). En conjunto, **61.28 %** de los hallazgos del mes cae en categorías de riesgo elevado, contra 54.65 % en julio. La superficie de exposición creció y se concentró en lo más grave.

Esta concentración de riesgos de alto impacto indica que las organizaciones enfrentan una presión considerable para priorizar y remediar un volumen creciente de amenazas inminentes. 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 cambio de composición más visible está en el ranking de productos. En julio el Top 10 estaba ocupado **exclusivamente** por versiones de Windows y Windows Server. En agosto lo encabeza `chrome` con 396 vulnerabilidades, casi el doble que el siguiente producto, `windows_server_2025` (215). El resto de la tabla sigue dominado por el ecosistema Microsoft —`windows_11_26h1` (199), `windows_11_24h2` y `windows_11_25h2` (196 cada uno), `windows_server_2022` (195)—, pero la irrupción del navegador en el primer lugar rompe el patrón sostenido del mes anterior y traslada parte del riesgo desde el sistema operativo hacia el punto de acceso web del usuario.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

Vectores de ataque recurrentes

El examen de las Críticas de agosto muestra un desplazamiento respecto de julio. El vector dominante ya no es solo la ejecución remota de código en aplicaciones web: aparece con fuerza el **compromiso de la cadena de distribución de software**. Destacan el compromiso del bucket oficial de actualizaciones de `MonsterInsights Pro`, con código malicioso en dos releases sucesivas, y varios complementos de WordPress que son directamente maliciosos —`Premium SEO`, `Link Factory`— con puertas traseras que crean cuentas de administrador ocultas.

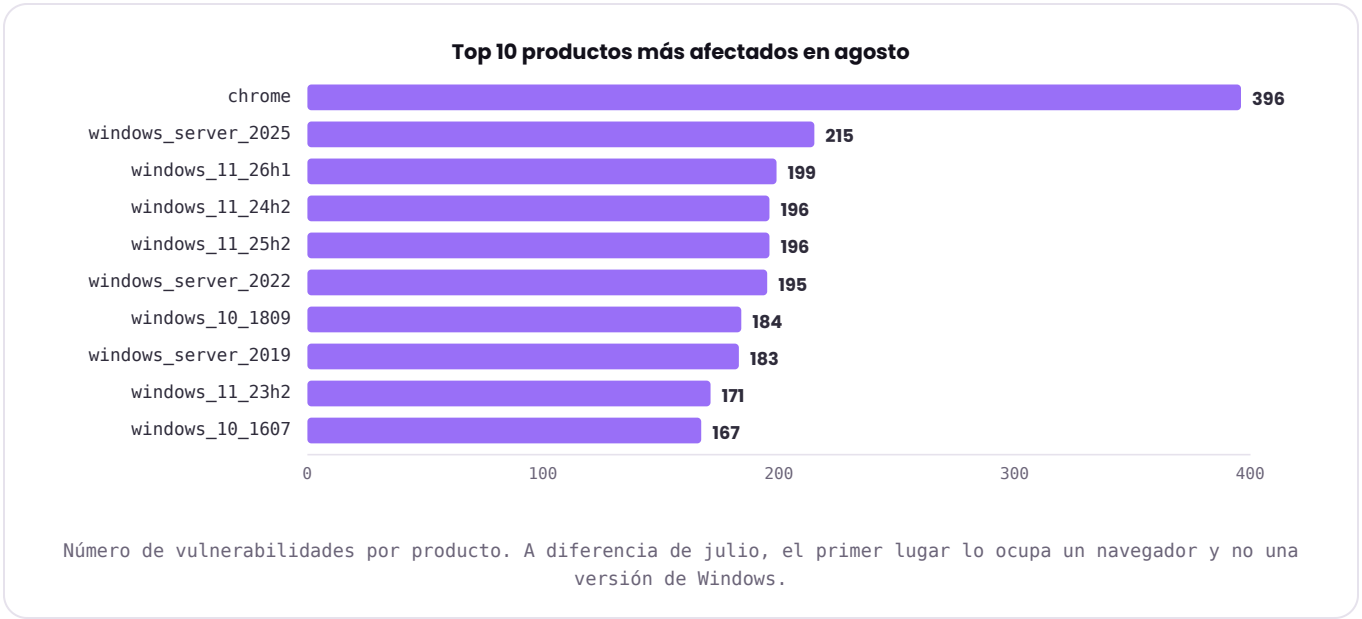
El **ecosistema WordPress y Joomla** concentra un número alto de RCE no autenticadas: `W3 Total Cache`, `Custom Fields`, `WP BASE Booking`, `Spider Analyser`, `Type Hub`, y en Joomla `Fabrik` y `Balbooa Forms`.

En **nube y plataformas gestionadas** el volumen es notable y casi todo corresponde a Microsoft: `Azure SQL Database`, `Azure SQL Managed Instance`, `Azure Arc`, `Azure Managed Instance for Apache Cassandra`, `Microsoft Entra ID`, `Microsoft Teams`, `Exchange Online` y `Planetary Computer Pro`, en general por autenticación o autorización deficiente, SSRF e inyección de argumentos.

La tendencia de **plataformas de IA y agentes** que ya se observaba en julio se consolida y cambia de forma. Ahora no solo aparecen fallos en los frameworks —`PraisonAI`, `Xinference`, `Kubeflow Pipelines`— sino en las plataformas comerciales que incorporan IA: tres vulnerabilidades críticas distintas en `ServiceNow AI Platform`, entre ellas un escape de sandbox. El caso de PraisonAI es particularmente ilustrativo porque el fallo está en el flujo de CI/CD que acompaña al proyecto, no en el producto.

En **aplicaciones empresariales** pesan `Adobe Campaign Classic` (cuatro Críticas), `Adobe ColdFusion`, `SAP Commerce Cloud`, `Oracle Fusion Middleware`, `Oracle Hyperion`, `IBM DOORS Next`, `IBM i` y `Dassault SIMULIA`.

Los **dispositivos industriales y de red** siguen expuestos por ausencia de autenticación: `SIMATIC IoT2050` con Node-RED sin credenciales, `Haiwell IoT Cloud HMI Gateway` con inyección de comandos, y una serie de correcciones preventivas de Cisco en `Crosswork` y `Secure Workload`. En el **kernel de Linux** se registran fallos en el manejo de GRO de Geneve y en las tablas FIB de IPv4.



Número de vulnerabilidades por producto. A diferencia de julio, el primer lugar lo ocupa un navegador y no una versión de Windows.

INTELIGENCIA DE SEGURIDAD · ORACLE · MICROSOFT · GOOGLE

Panorama Big Tech

Este reporte mensual de inteligencia resume las vulnerabilidades identificadas en productos de nuestros principales proveedores tecnológicos. El orden del mes anterior se invirtió por completo.

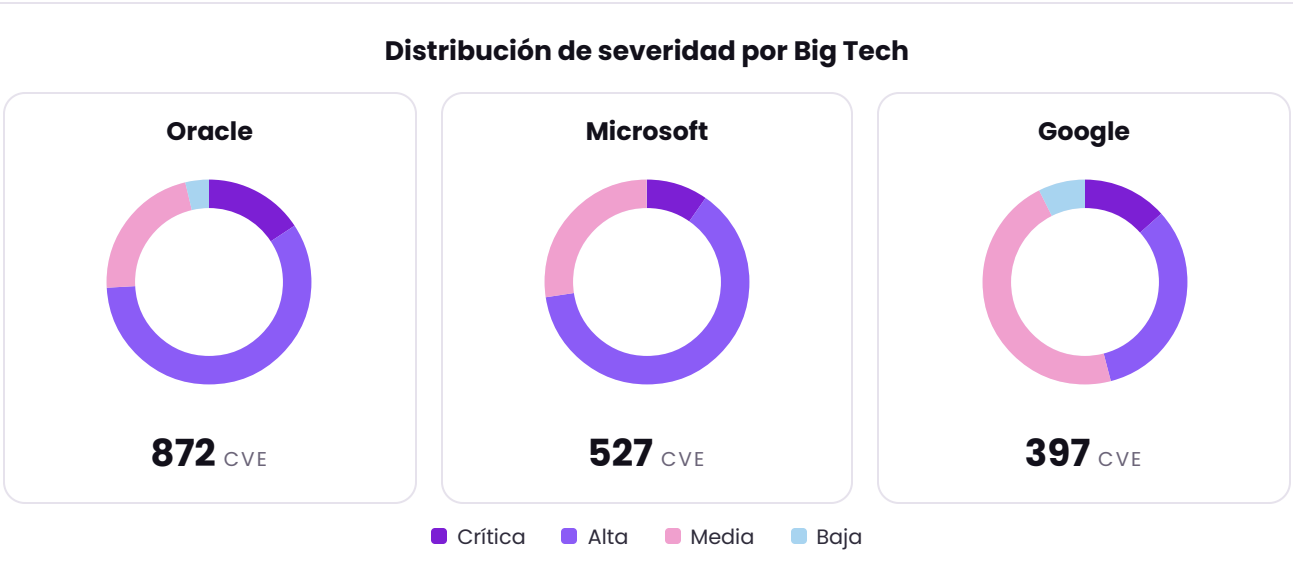
Oracle pasa a encabezar el volumen con **872 vulnerabilidades**: 137 Críticas, 508 Altas, 193 Medias y 34 Bajas. En julio registró 151, de modo que multiplicó por 5.8 su recuento y aporta el mayor número absoluto de hallazgos Críticos del grupo (137). La concentración se da en Fusion Middleware y Hyperion, con fallos explotables de forma remota y sin autenticación en componentes de directorio, gestión de identidad y consolidación financiera.

Microsoft baja de 708 a **527 vulnerabilidades**: 51 Críticas, 331 Altas, 144 Medias y 1 Bajas. Pese a la caída, mantiene el perfil más sesgado hacia la gravedad Alta: 331 de sus 527 hallazgos (63 %) caen en esa categoría, y solo 1 en Baja. El foco se desplazó del navegador Edge hacia los servicios gestionados de Azure y la plataforma de identidad.

Google sube de 249 a **397 vulnerabilidades**: 53 Críticas, 129 Altas, 185 Medias y 30 Bajas, y presenta la distribución más equilibrada de los tres, con el grueso en severidad Media (185). Se concentran predominantemente en el navegador Chrome, que además encabeza el Top 10 de productos del mes con 396 vulnerabilidades asociadas.

La lectura conjunta es que el riesgo de agosto se reparte de forma distinta a julio. Microsoft deja de ser el único foco relevante y aparecen dos concentraciones separadas: una en el *middleware* empresarial de Oracle, que afecta a sistemas de back office y de identidad corporativa, y otra en el navegador, que afecta al puesto de trabajo. Son dos superficies con perfiles de exposición y ventanas de parcheo muy distintas y conviene tratarlas por separado en la planificación de remediación.

Distribución de severidad por Big Tech



DISTRIBUCIÓN POR FABRICANTE

Severidad por marca

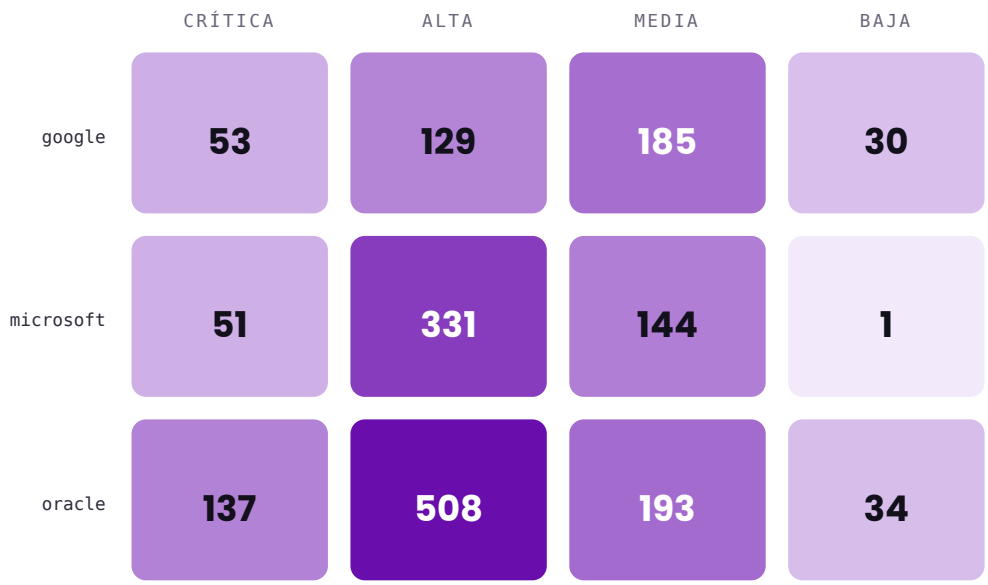
Conteo de vulnerabilidades por fabricante y nivel de severidad. La intensidad cromática representa el número de CVE por celda: Oracle concentra el grueso de los hallazgos de severidad Alta y también el mayor número de Críticas, mientras que Google presenta la mayor proporción relativa de hallazgos de severidad Media.

ORACLE
872
137 crít · 508 altas

MICROSOFT
527
51 crít · 331 altas

GOOGLE
397
53 crít · 129 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.

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.

CVE-2023-27350

EPSS 99.99 %

PaperCut MF y PaperCut NG: escalada de privilegios que permite a un atacante no autenticado omitir la autenticación y ejecutar comandos arbitrarios con privilegios SYSTEM.

EPSS alto: explotación activa por diversos actores, incluidos grupos de ransomware. Exploits públicos sobre sistemas de gestión de impresión ampliamente adoptados, con RCE no autenticada.

! 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, MDM, CI/CD y servidores de impresión—. Las organizaciones deben priorizar la aplicación de estos parches sin demora.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · CADENA DE SUMINISTRO

CVE-2026-11976

MonsterInsights Pro · Canal de actualización

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> El bucket oficial de distribución de actualizaciones de MonsterInsights Pro (`monster-insights.s3.amazonaws.com`) fue comprometido. Tanto la release vigente (10.2.2) como la versión 10.2.0 a la que el fabricante revirtió contienen un archivo malicioso, `class-system-check.php`.

1 VECTOR DE ATAQUE

No hay un fallo de software que explotar: el atacante controla el canal de distribución. Según el registro del NVD, se observaron tres variantes distintas el 11 de junio de 2026, todas con la misma clave AES-256-GCM, lo que apunta a un único actor, y el atacante conservaba acceso de escritura al bucket iterando la carga útil durante el día. Cualquier instalación que ejecute la actualización automática recibe el código malicioso desde una fuente legítima y firmada por el proveedor.

2 IMPACTO TÉCNICO

El código se ejecuta con los privilegios del proceso de WordPress. El cambio de alcance del vector CVSS (S:C) refleja que el compromiso trasciende el complemento y alcanza al sitio completo y a los datos que este maneja. La reversión a 10.2.0, que en circunstancias normales sería la mitigación correcta, también entrega código comprometido.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad porque neutraliza el control de seguridad más básico —mantener el software actualizado— y lo convierte en el vector de infección. Afecta a una base instalada amplia de sitios WordPress con analítica, muchos de ellos de cara al público. La respuesta no es parchear sino verificar integridad de archivos y asumir compromiso en toda instalación que haya actualizado en la ventana afectada.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-69836

Microsoft Entra ID

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Deserialización de datos no confiables en Microsoft Entra ID que permite a un atacante no autorizado ejecutar código a través de la red.

1 VECTOR DE ATAQUE

El registro del NVD identifica deserialización de datos no confiables. Esto implica que un componente del servicio reconstruye objetos a partir de datos que el atacante puede influir, sin validar el tipo ni el origen. El vector CVSS 3.1 AV:N/AC:L/PR:N/UI:N/S:C indica explotación por red, de baja complejidad, sin credenciales ni interacción del usuario, y con cambio de alcance. Microsoft no ha divulgado el endpoint afectado ni el formato de serialización involucrado.

2 IMPACTO TÉCNICO

Entra ID es el proveedor de identidad de la organización. La ejecución de código en ese contexto permitiría emitir o manipular tokens, alterar directivas de acceso condicional, crear o elevar principales de servicio y acceder a cualquier aplicación federada. El cambio de alcance confirma que el impacto se extiende más allá del componente vulnerable.

3 JUSTIFICACIÓN DEL RIESGO

Es la vulnerabilidad de mayor consecuencia potencial del mes para organizaciones con identidad en la nube. Con un EPSS de 1.56 % es, además, la crítica de Microsoft con mayor probabilidad estimada de explotación en agosto: un valor bajo en términos absolutos, pero unas tres veces superior a la mediana del conjunto crítico analizado. El compromiso del plano de identidad no se contiene con segmentación de red.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-61241

Oracle Internet Directory · OID LDAP Server

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · LDAP**

> Vulnerabilidad en el componente OID LDAP Server de Oracle Internet Directory, 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 LDAP comprometer el producto.

1 VECTOR DE ATAQUE

El propio aviso de Oracle califica la vulnerabilidad como de explotación sencilla, sin autenticación, a través de LDAP, 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 Internet Directory.

2 IMPACTO TÉCNICO

OID es el directorio de identidad corporativa sobre el que se apoyan las aplicaciones de Fusion Middleware. Su compromiso permite leer, modificar o eliminar entradas del directorio, incluidas cuentas, grupos y políticas, y potencialmente hashes de credenciales. Un atacante puede falsificar identidades y acceder a las aplicaciones que confían en el directorio.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad y repite el patrón que ya identificamos en julio con Oracle Unified Directory (CVE-2026-60360): el directorio de identidad como punto único de fallo, alcanzable sin credenciales desde la red. Si en julio se abrió un hallazgo por OUD, corresponde revisar si el mismo cliente opera OID y tratar ambos como un único riesgo de identidad.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-48362

Adobe ColdFusion

SEVERIDAD **Crítica**

EXPLOTABLE **sin interacción del usuario**

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

1 VECTOR DE ATAQUE

El aviso de Adobe 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 sin saneamiento suficiente.

2 IMPACTO TÉCNICO

Ejecución de código en el servidor de aplicaciones. ColdFusion suele desplegarse en el perímetro sirviendo aplicaciones de negocio, con conectividad hacia bases de datos internas, lo que lo convierte en un punto de pivote hacia la red corporativa.

3 JUSTIFICACIÓN DEL RIESGO

Con EPSS de 4.31 % es la vulnerabilidad crítica de agosto con mayor probabilidad estimada de explotación en el conjunto analizado, casi diez veces la mediana. ColdFusion tiene un historial extenso de explotación masiva tras la publicación del aviso, con varias entradas históricas en el catálogo KEV, lo que refuerza la urgencia aunque a la fecha de cierre no figure en KEV.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-56162

Microsoft Azure SQL Database

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Autenticación impropia en Azure SQL Database que permite a un atacante no autorizado elevar privilegios a través de la red.

1 VECTOR DE ATAQUE

El registro describe un fallo en el mecanismo de autenticación del servicio gestionado. El vector AV:N/AC:L/PR:N/UI:N/S:C indica que el ataque es remoto, de baja complejidad y no requiere credenciales previas ni interacción. El fabricante no ha publicado el detalle del mecanismo afectado.

2 IMPACTO TÉCNICO

Acceso no autorizado a bases de datos gestionadas y a los datos que contienen. El cambio de alcance sugiere que el impacto puede extenderse a recursos fuera de la instancia vulnerable dentro del entorno del inquilino.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica para cualquier organización con datos regulados en Azure SQL. En el contexto chileno, un acceso no autorizado a bases de datos con datos personales activa las obligaciones de la Ley 21.719, y en entidades supervisadas por la CMF puede constituir un incidente reportable. Corresponde verificar si la mitigación fue aplicada por Microsoft del lado del servicio o si requiere acción del inquilino.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-58231

SAP Commerce Cloud

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> SAP Commerce Cloud permite a un atacante no autenticado abusar de un cliente de autenticación por defecto y enviar entradas especialmente diseñadas a funciones que carecen de validación suficiente.

1 VECTOR DE ATAQUE

El aviso describe dos condiciones encadenadas: la existencia de un cliente de autenticación preconfigurado que el atacante puede usar, y funciones que no validan adecuadamente la entrada recibida. La combinación permite alcanzar código ejecutable sin credenciales legítimas.

2 IMPACTO TÉCNICO

Ejecución de código arbitrario y compromiso de componentes internos, con alto impacto en confidencialidad, integridad y disponibilidad de la aplicación. En una plataforma de comercio esto alcanza catálogo, precios, pedidos y datos de clientes.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por tratarse de una configuración por defecto: el sistema es vulnerable tal como se entrega, sin que medie un error de despliegue del cliente. Con EPSS de 1.71 % está entre las críticas con mayor probabilidad estimada del mes.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · INYECCIÓN DE CÓDIGO

CVE-2026-18885

ServiceNow AI Platform

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Inyección de código en la plataforma de IA de ServiceNow que, bajo determinadas circunstancias, permitiría a un usuario no autenticado ejecutar código arbitrario en la plataforma y acceder o modificar datos de la instancia más allá de lo previsto.

1 VECTOR DE ATAQUE

El fabricante no detalla el punto de inyección. El aviso acota la explotación a «determinadas circunstancias», lo que sugiere condiciones de configuración específicas. ServiceNow indica haber desplegado la actualización en instancias alojadas y haberla puesto a disposición de socios y clientes autogestionados, y declara no tener constancia de explotación maliciosa.

2 IMPACTO TÉCNICO

Ejecución de código dentro de la plataforma y acceso o modificación de datos de la instancia. ServiceNow concentra habitualmente inventario de activos, tickets, flujos de aprobación y datos de recursos humanos, de modo que el acceso indebido tiene alcance transversal.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y forma parte de un grupo de tres vulnerabilidades críticas distintas publicadas en agosto sobre la misma plataforma: esta inyección de código, un control de acceso impropio (CVE-2026-18886) y un escape de sandbox (CVE-2026-6876). La concentración de tres fallos independientes de puntuación 10.0 en un mismo producto en un solo mes es en sí misma una señal de riesgo sobre la madurez de la superficie de IA.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · INYECCIÓN DE COMANDOS EN CI/CD

CVE-2026-48168

PraisonAI · Flujo de GitHub Actions

SEVERIDAD **Crítica**

EXPLOTABLE **colaborador externo**

> En versiones anteriores a la 4.6.40, el flujo de GitHub Actions que acompaña a PraisonAI es vulnerable a inyección de comandos: incrusta el nombre de rama de un pull request controlado por el atacante dentro de un bloque `run:` de Bash sin comillas ni validación.

1 VECTOR DE ATAQUE

El flujo además permite que cualquier comentario `@claude` dispare el trabajo, sin comprobar si quien comenta es un colaborador de confianza. Un contribuyente externo puede abrir un pull request desde un fork cuyo nombre de rama contenga metacaracteres de shell y comentar para provocar la ejecución de código arbitrario en el runner.

2 IMPACTO TÉCNICO

Los comandos se ejecutan en un trabajo que sostiene un token de GitHub App con permisos de escritura, acceso OIDC y acceso a `gh` y `git`. La inyección puede encadenarse a través de `$GITHUB_PATH` para comprometer pasos privilegiados posteriores, habilitando escrituras en el repositorio, manipulación de pull requests e incidencias, o abuso del token OIDC. Corregido en 4.6.40.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y su valor para este informe excede al producto afectado. El patrón —nombre de rama sin sanear en un bloque de shell, más disparador abierto a cualquier comentario— es replicable en cualquier organización que haya incorporado flujos de automatización con IA a su CI/CD. Recomendamos usarla como caso de referencia para auditar los propios flujos, no solo para descartar el uso de PraisonAI.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-58115

Siemens SIMATIC IoT2050 Advanced · Node-RED

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · HTTP**

> Todas las versiones anteriores a la V4.3.4.1 del SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2) que ejecutan Industrial OS con Node-RED instalado no aplican autenticación en la interfaz HTTP de Node-RED.

1 VECTOR DE ATAQUE

La interfaz expone sin credenciales los nodos de programación, que son capaces de ejecutar comandos del sistema en el servidor. Un atacante remoto no autenticado puede crear flujos maliciosos a través de la interfaz HTTP.

2 IMPACTO TÉCNICO

Ejecución de código arbitrario en el servidor subyacente con privilegios máximos. En un gateway industrial esto significa control sobre la adquisición de datos de planta y un punto de entrada desde la red de TI hacia la red de operaciones.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por el emplazamiento del dispositivo más que por la sofisticación del fallo: no hay que explotar nada, basta con alcanzar la interfaz. Para clientes de infraestructura crítica sujetos a la Ley 21.663, un gateway OT accesible sin autenticación es un hallazgo de segregación de red además de uno de parcheo.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · PUERTA TRASERA

CVE-2026-14812

Complemento «Premium SEO» para WordPress

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> El complemento Premium SEO para WordPress es malicioso por diseño: incorpora una puerta trasera no autenticada que crea una cuenta de administrador oculta.

1 VECTOR DE ATAQUE

No se trata de una vulnerabilidad introducida por error sino de funcionalidad deliberada. En algunas compilaciones habilita además ejecución remota de código, server-side request forgery e inyección arbitraria de scripts y contenido en el front-end.

2 IMPACTO TÉCNICO

Control total del sitio afectado por parte de un atacante no autenticado. La cuenta de administrador oculta otorga persistencia que sobrevive a la desinstalación del complemento si no se audita la tabla de usuarios.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y, junto con el caso de MonsterInsights, define el patrón del mes: el riesgo no está solo en el código con errores sino en el código que nunca debió instalarse. Recomendamos incorporar al alcance de las evaluaciones un inventario de complementos con verificación de procedencia, y revisar la tabla de usuarios administradores en busca de cuentas no reconocidas.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

Agosto reveló un panorama más severo que julio, con **11,567 vulnerabilidades** y un 61.28 % concentrado en las categorías Crítica y Alta. Tres cambios estructurales definen el mes: Oracle desplaza a Microsoft como principal origen de hallazgos, el navegador sustituye al sistema operativo en la cabeza del ranking de productos, y la cadena de suministro de software deja de ser un riesgo teórico para materializarse en compromisos concretos de canales de distribución.

01 Priorizar por explotación confirmada, no solo por severidad

De las 1,818 vulnerabilidades Críticas del mes, apenas 15 tienen explotación confirmada en KEV. Ese subconjunto, junto con las 31 incorporaciones al catálogo durante agosto —siete de ellas de años anteriores—, debe encabezar la cola de remediación. Un puntaje CVSS de 10.0 sin señal de explotación no justifica desplazar una vulnerabilidad de 2015 que está siendo usada hoy.

02 Controlar la procedencia del software, no solo su versión

El compromiso del canal de actualización de MonsterInsights y los complementos maliciosos distribuidos como legítimos invalidan el supuesto de que actualizar es siempre seguro. Se requiere inventario de componentes de terceros, verificación de integridad de artefactos, control de procedencia antes de la instalación y capacidad de detectar cambios en archivos desplegados. Para clientes con desarrollo propio, el caso de PraisonAI muestra que el flujo de CI/CD es parte del perímetro.

03 Tratar el plano de identidad como un dominio de riesgo propio

Entra ID, Oracle Internet Directory y Azure SQL concentran fallos de autenticación y autorización explotables sin credenciales. El compromiso de un directorio de identidad no se contiene con segmentación de red ni con MFA en las aplicaciones, porque el atacante opera por encima de esos controles. Corresponde inventariar los proveedores de identidad en uso, reducir su exposición de red y definir un procedimiento de respuesta específico para su compromiso.

BASELINE

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

BOLETÍN DE VULNERABILIDADES · AGOSTO 2026