BASELINE

INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

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

PERIODO
Julio 2026

HALLAZGOS
9,919 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

9,919

VULNERABILIDADES DETECTADAS EN JULIO

Una cifra que subraya la constante evolución y expansión de la superficie de ataque global, con una composición marcadamente desplazada hacia amenazas de alto impacto.

CRÍTICAS	ALTAS	CRÍTICA + ALTA
1,307	4,114	5,421
13.17 % del total	41.48 % del total	54.65 % del total

El mes de julio presentó un panorama de ciberseguridad significativamente desafiante, con un total de **9,919 vulnerabilidades detectadas y divulgadas**. La distribución por nivel de criticidad es particularmente preocupante: **1,307 vulnerabilidades Críticas** (13.17 % del total) y **4,114 de gravedad Alta** (41.48 %). Esto significa que más de la mitad de las vulnerabilidades registradas este mes (**54.65 %**) corresponden a categorías de riesgo elevado, capaces de causar daños severos como ejecución remota de código, escalada de privilegios o exposición masiva de datos, a menudo sin requerir autenticación previa.

Esta concentración de riesgos de alto impacto indica que las organizaciones se enfrentan a una presión considerable para priorizar y remediar un gran volumen 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.

Una tendencia alarmante y persistente es la abrumadora concentración de vulnerabilidades en el ecosistema de Microsoft. El Top 10 de productos afectados está dominado **exclusivamente** por versiones de Windows y Windows Server: `windows_11_26h1` (395), `windows_11_24h2` y `windows_11_25h2` (392 cada uno) y `windows_server_2025` (389) encabezan la lista, seguidos de `windows_server_2022` (336), las ramas de `windows_10` (326, 326 y 322) y `windows_server_2019` (322) y `windows_server_2016` (259). Esta prevalencia resalta tanto su omnipresencia en entornos empresariales como el continuo atractivo que representan para los actores de amenazas: cualquier fallo de seguridad en estos productos puede tener un impacto sistémico en infraestructuras críticas a nivel mundial.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

Vectores de ataque recurrentes

Un examen detallado de las vulnerabilidades Críticas de julio revela un espectro amplio de vectores de alto impacto. La **Ejecución Remota de Código (RCE)** y la **Inyección SQL** dominan en plugins de WordPress (`WP-BusinessDirectory`, `SMS Alert`, `WPFunnels`), plataformas de gestión (`Control Web Panel`, `Mura CMS`, `SolarWinds Serv-U`, `Apache IoTDB`, `Apache Camel`) y aplicaciones empresariales (`Pivotal CRM`, `Bitwarden`, `Coolify`, `DbGate`).

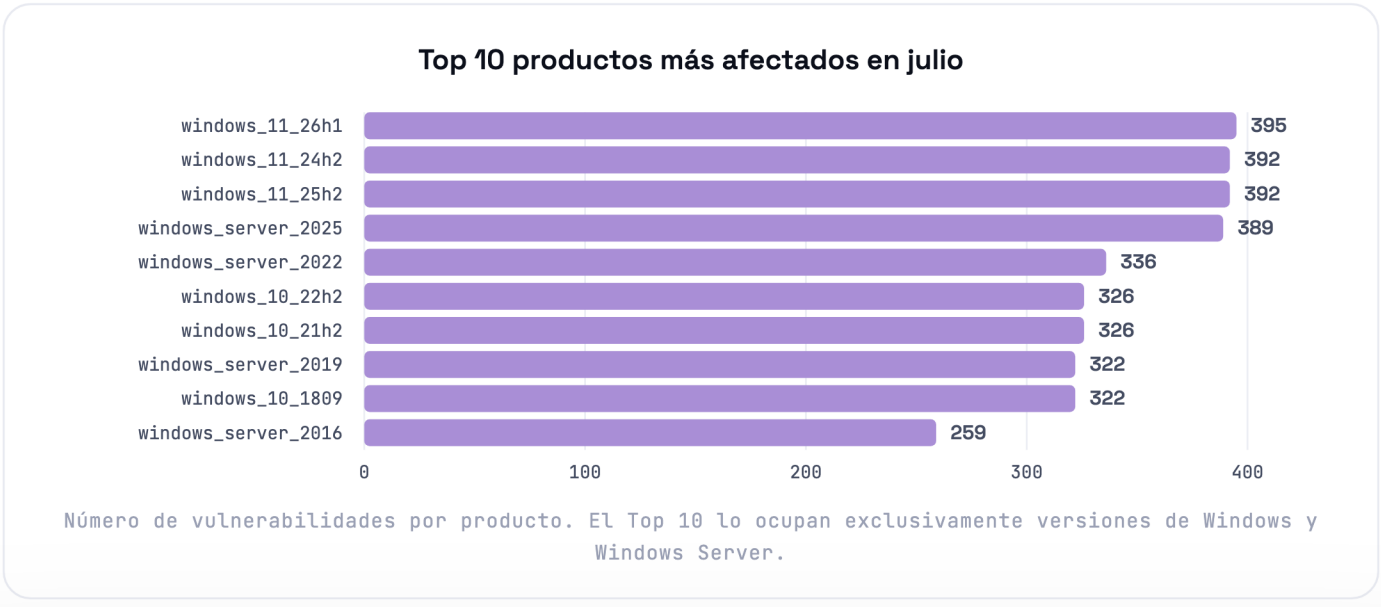
Las vulnerabilidades de **cadena de suministro y componentes de terceros** afectan a bibliotecas muy utilizadas (`containerd`, `libcurl`, `Gitea`, `Apache Thrift`, `node-tar`, `Docker Hub` y numerosos módulos de Perl), lo que implica un riesgo significativo y la necesidad de monitoreo constante de dependencias.

En **infraestructura cloud y contenedores** destacan fallos en `Kubernetes`, `Azure OpenAI`, `Azure Key Vault`, `AWS HealthLake` y `Google Cloud BigQuery`, en general por control de acceso, SSRF o gestión de credenciales. El **hardware y los dispositivos IoT/OT** siguen siendo un flanco débil: `UltraVNC repeater`, `WAGO System I/O`, cámaras `MERCURY` y cargadores `CHARX`, con contraseñas embebidas o ausencia de autenticación.

Una tendencia emergente y altamente preocupante son las múltiples vulnerabilidades en **frameworks y plataformas de IA y LLM**: `PraisonAI`, `Langroid`, `LocalAI`, `mem0`, `LightRAG`, `SGLang` y `h2oGPT`, con inyección de código, RCE, path traversal, SSRF y exposición de claves API. La rápida adopción de estas tecnologías está superando a las prácticas de seguridad.

Entre los **fallos fundamentales**, numerosas vulnerabilidades en el kernel de Linux, en componentes de `Google Chrome` (ANGLE, Skia, V8, GPU, WebGL) y en sistemas de Apple involucran corrupción de memoria — use-after-free, out-of-bounds, heap overflow, type confusion— que puede derivar en ejecución de código arbitrario o escalada a nivel de kernel.

Finalmente, la **autenticación y autorización deficientes** permite bypass, escalada de privilegios o acceso no autorizado en `BeyondTrust Remote Support`, `Check Point SmartConsole` y `VMware vCenter`, entre otros.



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, correspondiente al mes de julio, resume las vulnerabilidades críticas identificadas en productos de nuestros principales proveedores tecnológicos.

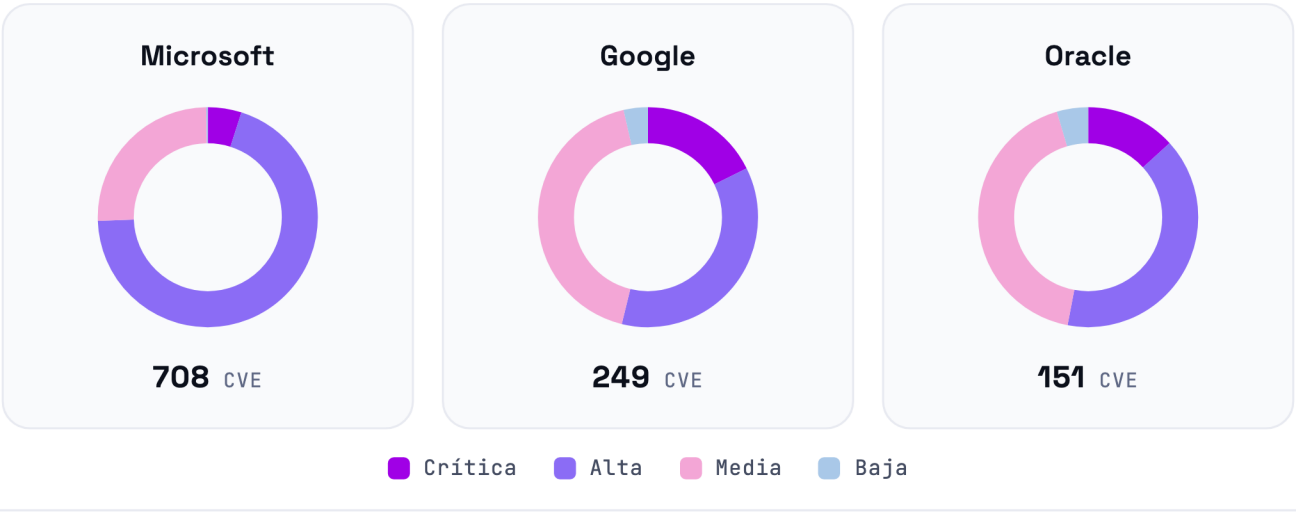
Microsoft presenta el mayor volumen total, con **708 vulnerabilidades**: 35 Críticas, 492 Altas, 179 Medias y 2 Bajas. Los hallazgos clave revelan una concentración de fallos en su navegador Edge basado en Chromium —use-after-free, heap-based buffer overflow e integer overflow o wraparound— todos con potencial de permitir la ejecución de código, en algunos casos por atacantes no autorizados y a través de la red.

Adicionalmente, se identificaron fallos en servicios de nube y aplicaciones empresariales, como una vulnerabilidad de **Server-Side Request Forgery (SSRF)** en Azure OpenAI y un problema de autorización incorrecta en Microsoft Exchange Online, ambas facilitando la elevación de privilegios sobre la red.

Google registró **249 vulnerabilidades**: 44 Críticas, 90 Altas, 106 Medias y 9 Bajas. Se concentran predominantemente en el navegador Chrome, afectando componentes como ANGLE, V8 y Skia. Su naturaleza abarca desde validación insuficiente de entradas no confiables e implementación inapropiada —que podrían llevar a escapes de sandbox y ejecución de código arbitrario por un atacante remoto— hasta heap buffer overflow e integer overflow que permiten acceso a memoria fuera de límites.

Oracle reportó **151 vulnerabilidades**: 20 Críticas, 60 Altas, 64 Medias y 7 Bajas, centradas en software empresarial y de virtualización. Destacan múltiples fallos en PeopleSoft Enterprise PeopleTools (PIA Core Technology, Process Scheduler, OpenSearch Dashboards) y en Oracle VM VirtualBox, en su componente Core. Estos hallazgos apuntan a una superficie de ataque asociada a la operación de sistemas críticos de negocio y entornos de virtualización.

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, mientras que Google presenta la mayor proporción relativa de hallazgos Críticos del grupo.

MICROSOFT
708
35 crít · 492 altas

GOOGLE
249
44 crít · 90 altas

ORACLE
151
20 crít · 60 altas

Mapa de calor por marca y severidad

	CRÍTICA	ALTA	MEDIA	BAJA
google	44	90	106	9
microsoft	35	492	179	2
oracle	20	60	64	7

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 zero-days.

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-2024-21887

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-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-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-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-2023-44487

EPSS 99.99 %

«HTTP/2 Rapid Reset Attack»: denegación de servicio que permite abrumar 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 —VPNs, MDM, CI/CD y servidores de impresión—. Las organizaciones deben priorizar la aplicación de estos parches sin demora.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-47056

Oracle Data Integrator · Servicio REST

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad explotable de forma remota y sin autenticación en el componente de Servicio REST de Oracle Data Integrator, que permite la toma de control completa de la instancia.

1 VECTOR DE ATAQUE

Un atacante puede interactuar con un endpoint HTTP vulnerable sin necesidad de credenciales ni interacción del usuario. El vector CVSS (AV:N/AC:L/PR:N/UI:N) sugiere un fallo en la validación de entrada, un error de deserialización, una inyección de comandos o un bypass de autenticación que permite la ejecución de código arbitrario. La baja complejidad de ataque facilita su explotación.

2 IMPACTO TÉCNICO

El impacto directo es la toma de control completa (RCE) de la instancia. Esto confiere al atacante la capacidad de manipular o exfiltrar datos que fluyen a través de los procesos ETL, modificar configuraciones de integración, introducir datos maliciosos en sistemas conectados o interrumpir por completo las operaciones. El cambio de alcance (S:C) es crítico: el compromiso de ODI puede impactar a bases de datos, data warehouses y otras aplicaciones interconectadas.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad: permite a un atacante no autenticado obtener control total sobre un componente neurálgico para la integración de datos empresariales. Puede resultar en filtraciones masivas de datos confidenciales, manipulación de registros financieros, interrupción de la cadena de suministro de datos y servir como punto de pivote para movimientos laterales en la red corporativa.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60217

Oracle Coherence · componente Core

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · TCP**

> Vulnerabilidad en el componente Core de Oracle Coherence que permite un ataque remoto y no autenticado a través de TCP, con toma de control completa de la instancia.

1 VECTOR DE ATAQUE

Dada la naturaleza de Coherence como caché distribuida en memoria, el vector más probable implica una vulnerabilidad de deserialización de objetos Java o una falla en el protocolo de comunicación de bajo nivel que permita la inyección de comandos o la ejecución de código arbitrario al procesar peticiones TCP maliciosas sin autenticación.

2 IMPACTO TÉCNICO

Un ataque exitoso conduce a la toma de control completa (RCE) de la instancia. El atacante puede ejecutar código arbitrario en los servidores Coherence, acceder, modificar o eliminar datos sensibles almacenados en la caché (sesiones de usuario, datos de aplicación), interrumpir la funcionalidad de las aplicaciones dependientes o introducir datos corruptos en el grid de datos. El cambio de alcance agrava el riesgo, ya que Coherence es fundamental para el rendimiento y la disponibilidad de numerosas aplicaciones.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por la capacidad de un atacante no autenticado de tomar el control total de una caché de datos en memoria empresarial. Puede llevar a una interrupción generalizada de servicios, la corrupción o exfiltración de datos sensibles en tiempo real y la ejecución de código que afecte directamente a las aplicaciones críticas que dependen de este servicio.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-60358

Oracle Access Manager · Motor de Autenticación

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad crítica en el Motor de Autenticación de Oracle Access Manager (OAM) que permite a un atacante no autenticado obtener acceso a través de HTTP.

1 VECTOR DE ATAQUE

El vector sugiere un bypass de autenticación severo: posiblemente una falla lógica en la verificación de credenciales, una inyección (SQL, LDAP o de comandos) en una fase pre-autenticación, o una deserialización de objetos Java en el proceso de autenticación que lleve a la ejecución remota de código. La facilidad de explotación y la ausencia de autenticación o interacción del usuario lo convierten en un objetivo primario.

2 IMPACTO TÉCNICO

El impacto es catastrófico: la toma de control completa de Oracle Access Manager. Un atacante puede eludir por completo los controles de autenticación y autorización, obtener privilegios administrativos, crear o modificar usuarios y roles, o acceder a cualquier aplicación protegida por OAM sin restricción. Equivale a obtener las llaves maestras de la gestión de identidades y accesos de la organización.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad. El compromiso de OAM otorga control total sobre la identidad y el acceso en toda la empresa: suplantación de cualquier usuario, incluidos administradores, acceso no autorizado a datos confidenciales y sistemas críticos, y capacidad de establecer persistencia en la propia infraestructura de seguridad.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60360

Oracle Unified Directory · OUD Core

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · LDAP**

> Vulnerabilidad en el componente OUD Core de Oracle Unified Directory, explotable de forma remota y sin autenticación a través de LDAP.

1 VECTOR DE ATAQUE

El vector más probable es una vulnerabilidad en el procesamiento de solicitudes LDAP no autenticadas: una inyección LDAP avanzada, una deserialización de datos maliciosos o un fallo de procesamiento de protocolo que permite la ejecución de código arbitrario antes de cualquier verificación de credenciales.

2 IMPACTO TÉCNICO

La consecuencia es la toma de control completa (RCE) de la instancia. Permite acceder, modificar o eliminar entradas de directorio, incluyendo información de usuarios, grupos, políticas de seguridad y potencialmente hashes de credenciales. Un atacante podría falsificar identidades, obtener acceso a otras aplicaciones que confían en OUD y controlar el libro de cuentas de la identidad corporativa.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica por la capacidad de un atacante no autenticado de obtener control total sobre el directorio de identidad central de la empresa. Puede manipular identidades, acceder a bases de datos de usuarios, escalar privilegios y controlar las políticas de acceso de una amplia gama de aplicaciones, con compromiso generalizado de cuentas, robo de datos y denegación de servicio.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60379

Oracle Service Delivery Platform · Messaging (SOAP)

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · SOAP**

> Vulnerabilidad en el componente Messaging Enabler de Oracle Service Delivery Platform, explotable remotamente y sin autenticación a través de SOAP.

1 VECTOR DE ATAQUE

Los vectores típicos incluyen inyección de entidades externas XML (XXE), fallos de deserialización de objetos Java dentro de payloads SOAP, o inyección de comandos a través de parámetros específicos en mensajes SOAP que son procesados sin una validación adecuada ni autenticación.

2 IMPACTO TÉCNICO

El resultado es la toma de control completa (RCE) de la instancia. Un atacante puede ejecutar código arbitrario, lo que le permitiría interceptar, modificar o falsificar comunicaciones críticas de mensajería, interrumpir flujos de trabajo de entrega de servicios y acceder a datos sensibles transmitidos por la plataforma. El cambio de alcance implica un posible efecto dominó en otros servicios que dependen de ella.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica: un atacante no autenticado puede obtener control total sobre una plataforma de entrega de servicios a través de su componente de mensajería. Esto puede llevar a la interrupción de procesos de negocio críticos, el robo o la manipulación de información sensible que transita por la plataforma, y su uso como punto de pivote hacia otros sistemas interconectados.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60389

Oracle Service Delivery Platform · Messaging (HTTP)

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · HTTP**

> Vulnerabilidad en el Messaging Enabler de Oracle Service Delivery Platform, explotable a través de HTTP sin autenticación, en el mismo componente que CVE-2026-60379.

1 VECTOR DE ATAQUE

Sugiere una ruta de ataque distinta a la del protocolo SOAP: posiblemente un endpoint HTTP expuesto, una interfaz web administrativa con bypass de autenticación, inyección de comandos en un formulario web o un fallo de deserialización en un servicio RESTful.

2 IMPACTO TÉCNICO

El impacto es idéntico al de CVE-2026-60379: la toma de control completa (RCE) de la instancia. El atacante obtendría la capacidad de ejecutar código arbitrario, interceptar, modificar o falsificar comunicaciones de mensajería, interrumpir flujos de trabajo y acceder a datos sensibles. La existencia de dos vectores críticos (SOAP y HTTP) en el mismo componente subraya la grave exposición.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica y, al igual que su CVE hermana, permite a un atacante no autenticado tomar el control completo de la plataforma, pero por una ruta HTTP. La presencia de múltiples vectores críticos en el mismo componente aumenta la superficie de ataque y la probabilidad de explotación, con las mismas consecuencias de interrupción de servicio y compromiso de datos.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60644

Oracle WebCenter Content · Web Content Management

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente Web Content Management de Oracle WebCenter Content, explotable de forma remota y sin autenticación a través de HTTP.

1 VECTOR DE ATAQUE

Los vectores comunes para RCE en sistemas de gestión de contenido incluyen la subida de archivos maliciosos (web shells) con bypass de restricciones, vulnerabilidades de deserialización en las interacciones de los componentes, inyecciones de comandos en funciones de búsqueda o manipulación de metadatos, o fallos de lógica que permiten la ejecución de código arbitrario.

2 IMPACTO TÉCNICO

El impacto es la toma de control completa (RCE) de la instancia. Un atacante puede ejecutar código arbitrario en el servidor, acceder, modificar o eliminar cualquier documento almacenado, desfigurar sitios web, inyectar código malicioso en el contenido servido a los usuarios, exfiltrar documentos confidenciales o usar el servidor como punto de apoyo para ataques internos.

3 JUSTIFICACIÓN DEL RIESGO

Es crítica: permite a un atacante no autenticado tomar el control total de un sistema central de gestión de contenido. Puede resultar en filtraciones masivas de información propietaria o datos personales, defacement de la presencia web de la empresa, distribución de malware a través de contenido comprometido y la interrupción completa de las operaciones de gestión de contenido.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-60366

Oracle Platform Security for Java · Thirdparty Jars

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «Centralized Thirdparty Jars» de Oracle Platform Security for Java, explotable de forma remota y sin autenticación a través de HTTP.

1 VECTOR DE ATAQUE

Sugiere un fallo en cómo la plataforma gestiona o carga JARs de terceros: posiblemente una deserialización de objetos en un servicio HTTP que procesa datos de entrada sin autenticación y luego intenta cargar o ejecutar código de JARs no validados. También podría tratarse de inyección de código o de una vulnerabilidad de «dependency confusion».

2 IMPACTO TÉCNICO

El impacto es la toma de control completa (RCE) de la plataforma. Como servicio de seguridad para aplicaciones Java, su compromiso permite ejecutar código arbitrario en un contexto de alta confianza: neutralizar los controles de seguridad de múltiples aplicaciones, inyectar código malicioso en aplicaciones críticas, manipular configuraciones de seguridad o acceder sin restricciones a los recursos gestionados.

3 JUSTIFICACIÓN DEL RIESGO

Es de máxima criticidad. El compromiso de una plataforma central de seguridad para aplicaciones Java socava directamente la postura de seguridad de una gran parte de la infraestructura basada en Java. Un atacante podría deshabilitar controles de seguridad, ejecutar código en sistemas de alta confianza y obtener acceso sin restricciones a datos y aplicaciones sensibles.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · AUTENTICACIÓN IMPROPIA

CVE-2026-56191

Microsoft Exchange Online

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Autenticación impropia en Microsoft Exchange Online que permite a un atacante no autorizado realizar manipulación de datos («tampering») a través de la red.

1 VECTOR DE ATAQUE

Implica una falla en el mecanismo de autenticación que permite la omisión o suplantación de identidad. Podría tratarse de un bypass lógico en el flujo de autenticación, una debilidad criptográfica en el manejo de tokens de sesión, o una vulnerabilidad que permita autenticarse como un usuario válido sin credenciales legítimas. El ataque es remoto y no requiere interacción del usuario.

2 IMPACTO TÉCNICO

Un atacante podría obtener acceso no autorizado a buzones de correo, leyendo, modificando o eliminando correos electrónicos, citas del calendario y contactos. Esto puede escalar a un compromiso completo de la cuenta, facilitando ataques de Business Email Compromise (BEC), exfiltración de información confidencial y campañas de phishing internas. El CVSS 10.0 indica que el impacto potencial va más allá del simple «tampering», pudiendo llegar al control total de cuentas.

3 JUSTIFICACIÓN DEL RIESGO

Es de riesgo crítico para cualquier empresa que utilice Exchange Online. Con un EPSS del 0.67 % existe una probabilidad real de explotación. El acceso no autorizado a los buzones es una vía directa para el robo de información confidencial, la suplantación de identidad para fraudes (BEC) y la propagación de malware a través de la infraestructura de correo.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-56163

Microsoft Azure Kubernetes Service (AKS)

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación · remoto**

> Falta de autenticación para una función crítica en Microsoft Azure Kubernetes Service que permite a un atacante no autenticado escalar privilegios a través de la red.

1 VECTOR DE ATAQUE

Un endpoint o servicio administrativo clave en AKS está expuesto sin ningún control de acceso. Un atacante puede invocar directamente esta función remota para obtener privilegios elevados dentro del clúster, sin credenciales ni interacción del usuario.

2 IMPACTO TÉCNICO

La elevación de privilegios en un clúster de Kubernetes equivale a obtener el control total del clúster. Un atacante con privilegios escalados puede desplegar cargas de trabajo arbitrarias, acceder a secretos y configuraciones sensibles (credenciales de base de datos, claves API), interrumpir aplicaciones y tomar control de los nodos subyacentes, con capacidad de ejecutar código remoto en el entorno de contenedores.

3 JUSTIFICACIÓN DEL RIESGO

Es extremadamente crítica para cualquier organización que dependa de AKS. Con un EPSS del 0.90 %, la probabilidad de explotación es baja pero el impacto es devastador: control administrativo sobre la plataforma de orquestación de contenedores, compromiso completo de todas las aplicaciones y datos alojados en el clúster, robo masivo de datos e interrupción de servicios.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

Julio reveló un panorama de ciberseguridad extremadamente desafiante, con una proliferación de **9,919 vulnerabilidades**, muchas de ellas críticas y de alta gravedad, y varias ya bajo explotación activa. La superficie de ataque se ha expandido notablemente para incluir plataformas de IA y LLM, mientras que los sistemas operativos y aplicaciones empresariales tradicionales siguen siendo objetivos primordiales. Esta situación exige una respuesta inmediata y una reevaluación estratégica de las defensas.

Para fortalecer nuestra postura de seguridad y mitigar estos riesgos inminentes, los equipos de TI empresariales deben priorizar las siguientes acciones:

01 **Priorización y aplicación agresiva de parches**

Implementar un régimen de gestión de parches agresivo y basado en el riesgo, priorizando la remediación inmediata de las vulnerabilidades con alto EPSS y las que impactan infraestructuras críticas como plataformas de acceso remoto, CI/CD y sistemas de gestión de identidad (Ivanti, Palo Alto, Oracle Access Manager). La velocidad de respuesta es crucial para neutralizar amenazas activamente explotadas.

02 **Fortalecimiento de nuevas superficies de ataque**

Fortalecer la seguridad de la cadena de suministro de software, los entornos cloud y la infraestructura de IA y LLM mediante controles estrictos de acceso, auditorías de dependencias y monitoreo continuo. La rápida evolución de los riesgos en IA exige directrices de seguridad adaptadas y proactivas para asegurar el desarrollo y despliegue de estas tecnologías.

03 **Refuerzo de controles fundamentales y defensa en profundidad**

Reforzar los controles de seguridad fundamentales mediante la segmentación de red, la implementación universal de autenticación multifactor (MFA), principios de mínimo privilegio y la integración de prácticas de desarrollo seguro. Esto es esencial para neutralizar vectores persistentes como RCE, inyección SQL y fallos de autenticación que afectan a una amplia gama de aplicaciones.

BASELINE

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

BOLETÍN DE VULNERABILIDADES · JULIO 2026