BASELINE

INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

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

PERIODO
Junio 2026

HALLAZGOS
8,001 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

8,001

VULNERABILIDADES DETECTADAS EN JUNIO

Un volumen sin precedentes de nuevos hallazgos, con una composición marcadamente desplazada hacia amenazas de alto impacto que exigen atención inmediata y prioritaria.

CRÍTICAS	ALTAS	MEDIAS	BAJAS
950	3,287	2,899	552
11.9 % del total	41 % del total	36 % del total	6.9 % del total

Durante el mes de junio, nuestro análisis identificó **8,001 vulnerabilidades**, con **950 clasificadas como Críticas** (≈11.9 %), **3,287 como Altas** (41 %), 2,899 como Medias (36 %) y 552 como Bajas (6.9 %). El recuento por severidad considera únicamente las categorías Crítica, Alta, Media y Baja; se excluyen del análisis las vulnerabilidades informativas o sin severidad asignada. Las categorías Crítica y Alta suman más del 50 % del total, lo que refleja una tendencia alarmante hacia amenazas de alto impacto: ejecución remota de código, escalada de privilegios, bypass de autenticación, denegación de servicio permanente y exfiltración masiva de datos.

Los principales fabricantes y proyectos afectados continúan siendo los pilares de la infraestructura digital: `chrome` (880), `macos` (592), `windows` (573) y `linux_kernel` (521) encabezan la lista, seguidos de `android` (222) y de múltiples versiones recientes de Windows (`windows_11_26h1`, `windows_server_2025`). Esta concentración confirma que los sistemas operativos fundamentales y las aplicaciones de uso diario siguen siendo vectores persistentes de ataque a escala global.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

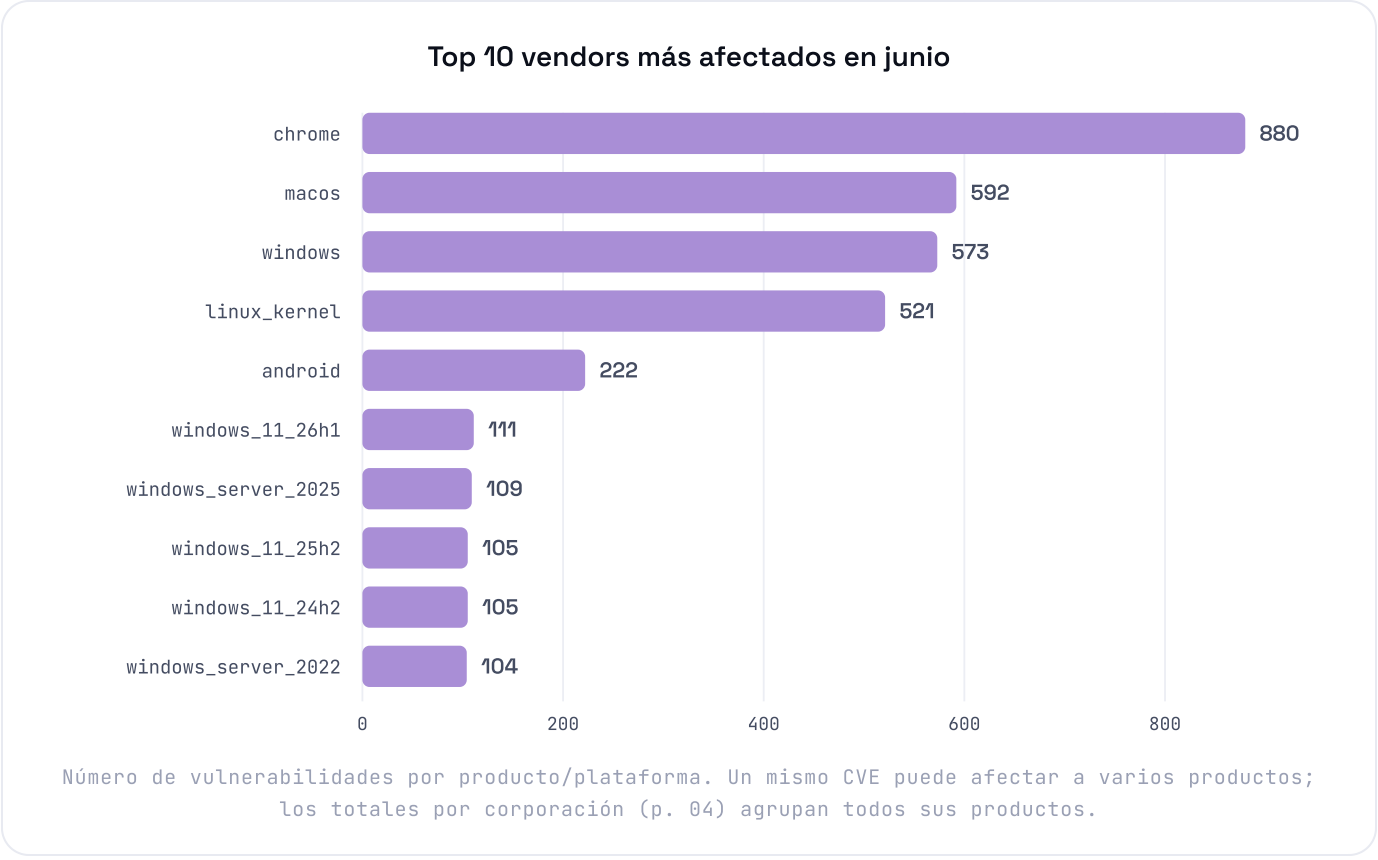
Vectores de ataque recurrentes

Un examen detallado de las vulnerabilidades Críticas de junio revela patrones alarmantes. La **Ejecución Remota de Código (RCE)** es la constante predominante, originada por validación inadecuada de entradas (`OTRS`, `Disig Web Signer`, `OpenMed`, `BashOperator` de Apache Airflow), deserialización de datos no confiables (`Teamwork Cloud`, `IBM WebSphere`, `Apache Fory`, `Nuance PowerScribe`) y desbordamientos de búfer (`Poly Voice`, `Windows TCP/IP` y `DHCP Client`).

Las vulnerabilidades de **Bypass de Autenticación** y **Escalada de Privilegios** siguen siendo una amenaza significativa: mecanismos de restablecimiento de contraseña inseguros (`ARMember`, `LoginPress Pro`, `Branda`), credenciales codificadas o débiles (`Aqara IAM/SSO`, `IBM Storage Protect`, `NetComm`) y controles de acceso faltantes (`Cloud Foundry UAA`, `authentik`, `Ivanti Sentry`, `FOSSBilling`).

La **Inyección SQL** continúa siendo una táctica efectiva y extendida en aplicaciones web y plugins (`WP Directory Kit`, `WP Job Portal`, `Open XDMoD`, `OSNexus QuantaStor`, `Raytha CMS`). También destacan las vulnerabilidades de **Path Traversal** y **carga/escritura de archivos arbitrarios**, que conducen a RCE o compromiso total (`Gravity Forms`, `Splunk Enterprise`, `Apache IoTDB`, `Budibase`, `Gitea act_runner`).

Las **vulnerabilidades de día cero** en componentes críticos, como los múltiples «use-after-free» y «out-of-bounds write» en `Google Chrome` —especialmente en ANGLE, GPU, FileSystem y WebGL— son particularmente graves, ya que permiten el escape del sandbox y la ejecución de código arbitrario. En conjunto, estos factores elevan la postura de riesgo global a un nivel **excepcionalmente crítico**.



Número de vulnerabilidades por producto/plataforma. Un mismo CVE puede afectar a varios productos; los totales por corporación (p. 04) agrupan todos sus productos.

INTELIGENCIA DE SEGURIDAD · MICROSOFT · GOOGLE · CISCO · ORACLE

Panorama Big Tech

El informe de junio detalla el panorama de vulnerabilidades críticas y de alto riesgo en tecnologías de Big Tech, con foco en Google, Microsoft, Cisco y Oracle.

Google presenta la mayor cantidad, con **1,007 vulnerabilidades**: 117 Críticas, 417 Altas, 448 Medias y 25 Bajas. La mayoría se centran en el ecosistema Android y servicios de aplicación, predominando la escalada local de privilegios y la fuga de información por falta de comprobaciones de permisos (CVE-2026-0072), validación de entrada inadecuada y errores lógicos.

Microsoft reportó **763 vulnerabilidades**: 59 Críticas, 404 Altas, 287 Medias y 13 Bajas. Entre los hallazgos clave, una inyección de comandos del SO en SharePoint (CVE-2026-47294) y una validación de entrada inadecuada en NI-PAL (CVE-2026-8036) que conduce a escalada local de privilegios.

Se observan además vulnerabilidades graves en componentes comúnmente integrados, como las relacionadas con ANGLE y Network en Google Chrome (CVE-2026-10881, CVE-2026-10882), que incluyen lecturas/escrituras fuera de límites, use-after-free y confusiones de tipo, permitiendo RCE y evasión de sandbox mediante páginas HTML maliciosas.

Oracle concentró **45 vulnerabilidades**: 11 Críticas, 23 Altas, 7 Medias y 4 Bajas, con la mayor proporción de hallazgos Críticos del grupo. Destacan tomas de control no autenticadas en Fusion Middleware (WebLogic, Coherence, WebCenter). **Cisco** reportó solo 2 vulnerabilidades (1 Alta, 1 Media), sin hallazgos Críticos este mes.

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: Google y Microsoft concentran el grueso de los hallazgos de severidad Alta y Media, mientras que Oracle presenta la mayor proporción relativa de hallazgos Críticos.

GOOGLE	MICROSOFT	ORACLE	CISCO
1,007	763	45	2
117 crít · 417 altas	59 crít · 404 altas	11 crít · 23 altas	0 crít · 1 alta

Mapa de calor por marca y severidad

	CRÍTICA	ALTA	MEDIA	BAJA
cisco	0	1	1	0
google	117	417	448	25
microsoft	59	404	287	13
oracle	11	23	7	4

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 del **100 %** y muchas han sido explotadas activamente como zero-days.

CVE-2024-3400 — 100.00 %

Palo Alto Networks PAN-OS: inyección de comandos que permite a un atacante no autenticado ejecutar código con privilegios de root. Afecta a gateways GlobalProtect con telemetría habilitada.

EPSS alto: explotada activamente como zero-day, exploits públicos y RCE sin autenticación en infraestructura de red crítica.

CVE-2024-21887 — 100.00 %

Ivanti Connect Secure y Policy Secure: inyección de comandos que permite a un administrador autenticado ejecutar comandos arbitrarios; suele encadenarse con otras vulnerabilidades.

EPSS alto: explotada como zero-day, combinada con CVE-2023-46805 para lograr RCE pre-autenticación en dispositivos VPN/NAC.

CVE-2024-23897 — 100.00 %

Jenkins CLI: lectura arbitraria de archivos que permite a un atacante no autenticado leer cualquier archivo del controlador Jenkins, con riesgo de divulgar información sensible.

EPSS alto: exploits públicos documentados sobre una plataforma CI/CD masiva, objetivo atractivo para exfiltración de credenciales.

CVE-2023-4966 — 100.00 %

Citrix NetScaler ADC y Gateway («Citrix Bleed»): divulgación de información que permite a un atacante no autenticado obtener datos sensibles de memoria y robar tokens de sesión.

EPSS alto: explotada de forma generalizada para secuestro de sesiones, con exploits públicos, en infraestructuras críticas de VPN.

CVE-2024-21893 — 100.00 %

Ivanti Connect Secure y Policy Secure: Server-Side Request Forgery (SSRF) que permite elaborar solicitudes especiales para acceder a recursos internos restringidos.

EPSS alto: parte de una cadena explotada activamente como zero-day por grupos APT contra infraestructuras VPN/NAC críticas.

CVE-2023-44487 — 100.00 %

«HTTP/2 Rapid Reset»: denegación de servicio que explota una debilidad del protocolo HTTP/2, generando y cancelando rápidamente un gran volumen de solicitudes para abrumar los servidores.

EPSS alto: usada en campañas a gran escala; afecta a cualquier servidor con HTTP/2 y es fácil de explotar, amenazando la disponibilidad.

CVE-2023-35082

100.00 %

Ivanti Endpoint Manager Mobile (EPMM): omisión de autenticación que permite a un atacante no autenticado eludir la autenticación y acceder a endpoints API sensibles del dispositivo.

EPSS alto: explotada como zero-day; acceso no autenticado a sistemas críticos de gestión de dispositivos móviles (MDM), con exploits públicos.

CVE-2023-32315

100.00 %

Openfire: path traversal que permite a un atacante no autenticado acceder a archivos restringidos vía un servlet de configuración, exponiendo configuraciones y, potencialmente, RCE.

EPSS alto: explotada activamente con exploits públicos, sobre un servidor de comunicaciones en tiempo real ampliamente usado.

CVE-2023-35078

100.00 %

Ivanti Endpoint Manager Mobile (EPMM): escritura arbitraria de archivos autenticada que permite a un atacante escribir archivos arbitrarios en el dispositivo.

EPSS alto: explotada como zero-day, a menudo encadenada con CVE-2023-35082 para lograr RCE no autenticado en infraestructuras MDM.

CVE-2023-27350

100.00 %

PaperCut MF/NG: omisión de autenticación que permite a un atacante no autenticado eludir la autenticación y obtener acceso administrativo total al servidor.

EPSS alto: explotada activamente con exploits públicos, sobre software de gestión de impresión en entornos sensibles, con control administrativo.

! URGENCIA DE PARCHEO, CRÍTICO Y EXTREMO

Todas las CVE listadas presentan un score EPSS del 100 %, lo que indica una probabilidad de explotación en la naturaleza extremadamente alta. Afectan a servicios y dispositivos críticos —VPNs, firewalls, plataformas CI/CD, MDM, servidores web y de impresión— y muchas han sido explotadas activamente como zero-days por actores avanzados, resultando en RCE, filtración de datos o DoS. Se requiere acción inmediata para identificar y remediar cualquier activo afectado.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ESCALADA LOCAL DE PRIVILEGIOS

CVE-2026-0072

Google Android · InputMethodManagerService

SEVERIDAD **Crítica**

ACCESO **local · sin interacción**

> Ausencia de verificación de permisos en la función `addInputMethodListener` del componente `InputMethodManagerService` de Android, que permite una escalada local de privilegios.

1 VECTOR DE ATAQUE

La vulnerabilidad reside en la función `addInputMethodListener` de `com.android.server.inputmethod.InputMethodManagerService`. La ausencia de una verificación de permisos adecuada permite que una aplicación local, con privilegios bajos y sin interacción del usuario ni permisos adicionales, invoque esta función de forma ilegítima y manipule el servicio para realizar acciones que normalmente requerirían permisos elevados.

2 IMPACTO TÉCNICO

El impacto primario es una escalada de privilegios local (LPE). El atacante podría acceder a recursos o realizar operaciones que exceden los permisos de su proceso original, comprometiendo la seguridad y la privacidad de los datos del usuario o del sistema operativo a nivel local.

3 JUSTIFICACIÓN DEL RIESGO

Para una empresa, esta LPE en un sistema operativo móvil es crítica: una aplicación maliciosa instalada en un dispositivo corporativo podría eludir restricciones de seguridad y acceder a datos sensibles o funcionalidades administrativas. La explotación sin interacción del usuario y sin privilegios adicionales la hace altamente atractiva para lograr persistencia o lateralización dentro de un dispositivo comprometido.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-48567

Microsoft Azure HorizonDB

SEVERIDAD **Crítica** EPSS **0.97 %**

> Bypass de autenticación por suplantación (spoofing) en Azure HorizonDB que permite a un atacante no autorizado elevar privilegios a través de la red.

1 VECTOR DE ATAQUE

Un atacante no autorizado puede manipular metadatos o protocolos de comunicación para simular ser una entidad o cliente legítimo del servicio HorizonDB, eludiendo los mecanismos de autenticación de la red. Esto puede implicar el uso de credenciales falsificadas, tokens de sesión manipulados o errores en la validación de la identidad del cliente/servidor.

2 IMPACTO TÉCNICO

El atacante logra una elevación de privilegios sobre la red, obteniendo acceso no autorizado a los datos y recursos gestionados por Azure HorizonDB. Esto puede resultar en control total sobre la base de datos, exfiltración de información sensible, manipulación de datos o interrupción del servicio.

3 JUSTIFICACIÓN DEL RIESGO

Un bypass de autenticación en una base de datos en la nube permite acceso no autenticado y toma de control directamente desde la red —un escenario que conduce a una brecha masiva de datos e interrupción del negocio. El score EPSS del 0.97 % indica que, aunque no se ha detectado explotación, existe una probabilidad no despreciable de que sea explotada en el futuro.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-48303

Adobe Campaign Classic (ACC)

SEVERIDAD **Crítica** EPSS **0.55 %**

> Autorización incorrecta (Incorrect Authorization) en Adobe Campaign Classic 7.4.3 build 9394 y anteriores que permite ejecutar código arbitrario sin interacción del usuario.

1 VECTOR DE ATAQUE

ACC no valida correctamente los permisos de un usuario o entidad que intenta realizar una acción. Aprovechando esta falla, un atacante puede enviar solicitudes maliciosas al servidor que, debido a la autorización deficiente, son procesadas como si provinieran de un usuario con mayores privilegios o con autorización para ejecutar comandos del sistema, sin interacción del usuario.

2 IMPACTO TÉCNICO

La consecuencia directa es la ejecución de código arbitrario (RCE). Dado que el alcance ha cambiado («Scope changed»), el impacto puede extenderse más allá del componente afectado hacia sistemas interconectados. La RCE permite tomar el control total del servidor de ACC, instalar malware, exfiltrar datos o pivotar hacia otros sistemas de la red.

3 JUSTIFICACIÓN DEL RIESGO

Para las empresas que dependen de Adobe Campaign Classic en sus operaciones de marketing y datos de clientes, esta RCE es catastrófica: acceso a bases de datos de clientes, envío de comunicaciones fraudulentas y compromiso de la reputación de marca. El score EPSS del 0.55 % sugiere una probabilidad moderada de explotación futura.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-35292

Oracle WebLogic Server · Fusion Middleware

SEVERIDAD **Crítica** EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «Console» de WebLogic Server (14.1.2.0.0 y 15.1.1.0.0), fácilmente explotable por un atacante no autenticado con acceso HTTP a la red.

1 VECTOR DE ATAQUE

Un atacante no autenticado con acceso de red vía HTTP puede explotarla con baja complejidad. Típicamente implica una falla en la autenticación o autorización inicial de la consola —deserialización insegura, bypass de autenticación en la URL o una inyección que permite ejecutar código sin credenciales. El vector CVSS (AV:N/AC:L/PR:N/UI:N) confirma accesibilidad de red, baja complejidad y ausencia de autenticación e interacción.

2 IMPACTO TÉCNICO

Un ataque exitoso resulta en la toma de control total de WebLogic Server: leer, modificar o eliminar datos sensibles, alterar la configuración o el código, y denegar el acceso a usuarios legítimos. El cambio de alcance («Scope changed») implica que el compromiso puede impactar a otros productos o servicios interconectados que dependen de esta instancia.

3 JUSTIFICACIÓN DEL RIESGO

WebLogic Server es un componente central en muchas arquitecturas empresariales para alojar aplicaciones Java EE. Su compromiso puede llevar a una brecha de datos masiva, interrupción de servicios críticos, robo de propiedad intelectual y un impacto financiero y reputacional severo.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-35301

Oracle WebLogic Server · Fusion Middleware

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «Console» de WebLogic Server (12.2.1.4.0 y 14.1.1.0.0), fácilmente explotable por un atacante no autenticado con acceso HTTP a la red.

1 VECTOR DE ATAQUE

De naturaleza idéntica a CVE-2026-35292, con el mismo vector CVSS (AV:N/AC:L/PR:N/UI:N). Sugiere una falla fundamental en la capa de seguridad de la consola que permite el acceso y control sin credenciales a un atacante remoto no autenticado.

2 IMPACTO TÉCNICO

La explotación resulta en una toma de control completa del WebLogic Server afectado, con impacto total en Confidencialidad, Integridad y Disponibilidad. El atacante puede ejecutar código arbitrario, acceder a los datos de las aplicaciones alojadas, alterar su funcionamiento o deshabilitarlas. El cambio de alcance reitera la posibilidad de comprometer productos adicionales.

3 JUSTIFICACIÓN DEL RIESGO

Que un atacante no autenticado tome el control de un servidor WebLogic es un riesgo máximo. Estos servidores manejan aplicaciones críticas de negocio y datos financieros o de clientes; su interrupción o la exfiltración de datos puede acarrear multas regulatorias, pérdida de confianza y graves daños económicos.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-35307

Oracle Coherence · componente «Core»

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «Core» de Oracle Coherence (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 y 15.1.1.0.0), fácilmente explotable por un atacante no autenticado con acceso HTTP.

1 VECTOR DE ATAQUE

Indica una debilidad en la implementación principal de Coherence, posiblemente en el manejo de solicitudes entrantes, la serialización/deserialización de objetos o la comunicación de clúster, permitiendo la ejecución de comandos arbitrarios sin autenticación. El vector CVSS (AV:N/AC:L/PR:N/UI:N) subraya la facilidad de explotación remota y sin credenciales.

2 IMPACTO TÉCNICO

Coherence es una solución de caché de datos en memoria distribuida y de alta disponibilidad. La explotación conduce a su toma de control total: manipular los datos en caché, inyectar código malicioso en el clúster o interrumpir el servicio, afectando directamente a las aplicaciones que dependen de él. El cambio de alcance implica compromiso indirecto de otros productos.

3 JUSTIFICACIÓN DEL RIESGO

Coherence se usa para escalar aplicaciones críticas que manejan grandes volúmenes de datos transaccionales o de sesión. Su toma de control puede corromper datos operativos, robar información en memoria, denegar servicio a aplicaciones de misión crítica e interrumpir significativamente las operaciones del negocio.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-35308

Oracle Coherence · «Centralized Third Party Jars»

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «Centralized Third Party Jars» de Oracle Coherence, fácilmente explotable por un atacante no autenticado con acceso HTTP a la red.

1 VECTOR DE ATAQUE

Sugiere una debilidad en cómo Coherence maneja o carga librerías de terceros, o cómo expone funcionalidades a través de ellas. Un atacante no autenticado puede inyectar payloads maliciosos procesados por las librerías vulnerables o aprovechar una configuración defectuosa para lograr la ejecución de código. El vector CVSS es idéntico al de CVE-2026-35307.

2 IMPACTO TÉCNICO

La consecuencia es la toma de control completa de Oracle Coherence: control sobre el clúster de caché, manipulación de datos, ejecución de comandos arbitrarios en los nodos o interrupción del servicio, con impacto total en Confidencialidad, Integridad y Disponibilidad. El cambio de alcance significa que el impacto puede propagarse a otros productos que integran Coherence.

3 JUSTIFICACIÓN DEL RIESGO

El riesgo es idéntico al de CVE-2026-35307. La toma de control de un componente tan central para la gestión de datos distribuidos puede paralizar las operaciones empresariales, comprometer datos críticos en tiempo real y tener un impacto devastador en la continuidad del negocio y la reputación.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-46778

Oracle WebCenter Enterprise Capture · RMI

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el «Client Bundle» de Oracle WebCenter Enterprise Capture (12.2.1.4.0 y 14.1.2.0.0), fácilmente explotable por un atacante no autenticado con acceso RMI.

1 VECTOR DE ATAQUE

Una falla en el servicio RMI (Java Remote Method Invocation) expuesto por Enterprise Capture: falta de autenticación en el registro RMI, deserialización insegura de objetos pasados por RMI o exposición de métodos con permisos excesivos. El vector CVSS (AV:N/AC:L/PR:N/UI:N) confirma explotabilidad remota, sin autenticación ni interacción.

2 IMPACTO TÉCNICO

Un ataque exitoso resulta en la toma de control total de Enterprise Capture, usado para la digitalización y procesamiento de documentos. El atacante podría acceder a documentos confidenciales, modificar flujos de captura, inyectar documentos maliciosos o comprometer la integridad del proceso documental. El cambio de alcance implica riesgo para sistemas de gestión de contenido o bases de datos interconectadas.

3 JUSTIFICACIÓN DEL RIESGO

Por la sensibilidad de los datos que maneja, su compromiso es crítico: exfiltración de información confidencial (contratos, datos de clientes, documentos financieros), manipulación de registros e interrupción de procesos esenciales, con graves implicaciones regulatorias y de cumplimiento.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-46781

Oracle WebCenter Enterprise Capture · RMI

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el «Client Bundle» de Oracle WebCenter Enterprise Capture, de explotación fácil por un atacante no autenticado con acceso RMI a la red.

1 VECTOR DE ATAQUE

De manera idéntica a CVE-2026-46778, reside en el «Client Bundle» con el mismo patrón de debilidad en la interfaz RMI, posiblemente en un método o servicio distinto. El vector CVSS es idéntico (AV:N/AC:L/PR:N/UI:N): remoto, sin autenticación ni interacción del usuario.

2 IMPACTO TÉCNICO

La consecuencia directa es la toma de control total de Oracle WebCenter Enterprise Capture. El atacante obtiene el mismo nivel de control y acceso a los documentos y flujos de trabajo de captura, con impacto total en Confidencialidad, Integridad y Disponibilidad. El cambio de alcance sugiere que la explotación podría impactar a otros productos y sistemas empresariales.

3 JUSTIFICACIÓN DEL RIESGO

El riesgo es el mismo que para CVE-2026-46778. Que un atacante remoto y no autenticado tome el control de un sistema que gestiona información corporativa sensible representa una amenaza extrema de brecha de datos, interrupción operativa y daño reputacional.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · TOMA DE CONTROL

CVE-2026-46798

Oracle WebCenter Sites · CMS empresarial

SEVERIDAD **Crítica**

EXPLOTABLE **sin autenticación**

> Vulnerabilidad en el componente «WebCenter Sites» de Oracle WebCenter Sites (12.2.1.4.0 y 14.1.2.0.0), fácilmente explotable por un atacante no autenticado con acceso HTTP.

1 VECTOR DE ATAQUE

Sugiere una vulnerabilidad crítica en la aplicación web del CMS —inyección de código, deserialización o bypass de autenticación— que permite la ejecución de comandos en el servidor. El vector CVSS (AV:N/AC:L/PR:N/UI:N) confirma que no se necesita autenticación ni interacción del usuario.

2 IMPACTO TÉCNICO

La explotación resulta en la toma de control total de WebCenter Sites: acceso y modificación de contenido web, inyección de scripts maliciosos (XSS persistente), redirección de usuarios, desfiguración del sitio, robo de datos de sesiones o uso del servidor como pivote para ataques internos. El cambio de alcance indica que el compromiso puede afectar a otros sistemas.

3 JUSTIFICACIÓN DEL RIESGO

La toma de control de un CMS de nivel empresarial es crítica para la reputación de la marca: un atacante puede alterar el contenido público, desinformar a los clientes o realizar phishing. Además, el acceso a las bases de datos de contenido podría exponer información sensible y derivar en una brecha de datos con consecuencias financieras y legales.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

El mes de junio de 2026 reveló un paisaje de ciberseguridad excepcionalmente crítico, marcado por un volumen sin precedentes de **8,001 vulnerabilidades** de alta y crítica severidad. La recurrencia de vectores como la Ejecución Remota de Código y los bypass de autenticación, junto a la explotación activa de múltiples zero-days en sistemas operativos, navegadores y aplicaciones empresariales, exige una respuesta de seguridad inmediata y robusta para proteger nuestros activos esenciales.

Ante este escenario, es imperativo que nuestros equipos de TI empresariales adopten las siguientes recomendaciones accionables:

01 **Priorización extrema de parcheo**

Implementar un régimen de parches acelerado, con prioridad absoluta para las vulnerabilidades con EPSS del 100 % y explotación activa (Palo Alto Networks, Ivanti, Citrix, Jenkins y PaperCut). Incluye la actualización urgente de sistemas operativos, navegadores, middleware empresarial (Oracle WebLogic, Coherence), plataformas CI/CD y dispositivos de red y seguridad.

02 **Refuerzo de la postura y hardening**

Revisar y endurecer proactivamente las configuraciones de seguridad en toda la infraestructura crítica. Prestar atención especial a los mecanismos de autenticación, control de acceso y gestión de credenciales para mitigar bypass y escaladas de privilegios, en particular en Azure HorizonDB, Adobe Campaign Classic y los productos Oracle Fusion Middleware.

03 **Inteligencia de amenazas y respuesta a zero-days**

Fortalecer la integración de fuentes de inteligencia, como el modelo EPSS, para anticipar y responder ágilmente a vulnerabilidades de día cero y de alta probabilidad de explotación. Desarrollar y probar planes de respuesta para contener y remediar rápidamente estos ataques, minimizando el tiempo de exposición y el impacto potencial.

BASELINE

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

BOLETÍN DE VULNERABILIDADES · JUNIO 2026