INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W35 · 24 ago 2026 – 30 ago 2026

Boletín de Ciberseguridad

Resumen semanal de amenazas priorizadas, en español y con acciones claras.

RESUMEN EJECUTIVO

Esta semana, el Boletín de Ciberseguridad destaca una serie de vulnerabilidades críticas bajo explotación activa que exigen atención inmediata. Se han identificado fallos de control de acceso en Oracle HTTP Server y Oracle Weblogic Server (CVE-2026-21962) con CVSS 10.0, así como vulnerabilidades de ejecución remota de código en Microsoft SQL Server (CVE-2019-1068) y un fallo de autenticación en ownCloud (CVE-2023-49105) que permite acceso no autenticado a archivos. Adicionalmente, se alertan sobre explotaciones activas en Zimbra Collaboration (CVE-2026-73570) y Gitea (CVE-2026-60004). En el ámbito del malware, se han detectado campañas que distribuyen el backdoor RedC2 4.0 a través de paquetes npm maliciosos, así como nuevas amenazas Android como 'Manic' y malware en sistemas de infoentretenimiento vehicular.

3 Crítica 6 Alta

Publicado 31 ago 2026

Fuentes: CISA KEV, NVD y avisos de fabricante.

Ver detalle →

NIT: 816007833-0
Pereira, Colombia
+57 314 682 5259
ingenieriatelematica.com.co

VISTA RÁPIDA

Severidad CVSS · explotación activa (CISA KEV)

3	6	0	0
Crítica	Alta	Media	Baja

9 vulnerabilidades con explotación activa confirmada · 4 campaña(s) de malware · 4 noticia(s)

VULNERABILIDADES

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2023-49105

ownCloud Improper Authentication Vulnerability

ownCloud ownCloud · · Versiones afectadas: -

Fallo de autenticación inapropiada en ownCloud que permite el acceso y manipulación de archivos sin autenticación.

Impacto: Un atacante puede acceder, modificar o eliminar cualquier archivo si conoce el nombre de usuario de una víctima y esta no tiene configurada una clave de firma.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad disponibles a más tardar el 2026-08-30.

Ampliar información: NVD — CVE-2023-49105 CISA KEV

Crítica · CVSS 0.0 EXPLOTACIÓN ACTIVA CVE-2026-73570

Vulnerabilidad de ejecución remota de código en Zimbra Collaboration

Zimbra Collaboration · · Versiones afectadas:

Falla de ejecución remota de código (RCE) en Zimbra Collaboration que está siendo explotada activamente.

Impacto: Permite a un atacante ejecutar código arbitrario en el servidor afectado, comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

> **Acción a seguir:** Revisar la infraestructura de Zimbra y aplicar los parches de seguridad recomendados de inmediato para mitigar la vulnerabilidad.

Ampliar información: NVD — CVE-2026-73570 CISA KEV

Crítica · CVSS 0.0 EXPLOTACIÓN ACTIVA CVE-2026-60004

Vulnerabilidad crítica RCE en Gitea bajo explotación activa

Gitea · · Versiones afectadas:

Vulnerabilidad crítica de ejecución remota de código (RCE) en Gitea, explotada activamente para desplegar cargas tipo minero de criptomonedas.

Impacto: Un atacante puede ejecutar código arbitrario en el servidor Gitea, lo que lleva a la implementación de cargas maliciosas como mineros de criptomonedas y un compromiso total del sistema.

> **Acción a seguir:** Aplicar los parches de seguridad para Gitea con urgencia.

Ampliar información: NVD — CVE-2026-60004 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2019-1068

Microsoft SQL Server Remote Code Execution Vulnerability

Microsoft SQL Server · · Versiones afectadas: `unspecified; 2017 for x64-based Systems (CU)`

Vulnerabilidad de ejecución remota de código en Microsoft SQL Server.

Impacto: Un atacante podría ejecutar código en el contexto de la cuenta de servicio de SQL Server Database Engine, lo que podría conducir a un control completo del servidor de base de datos.

> **Acción a seguir:** Aplicar las actualizaciones para Microsoft SQL Server 2017 para sistemas basados en x64 (CU) a más tardar el 2026-08-29.

Ampliar información: NVD — CVE-2019-1068 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2026-8452

Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Citrix NetScaler ADC and NetScaler Gateway · · Versiones afectadas: `14.1 – <72.61; 13.1 – <63.18; 14.1 FIPS – <72.61; 13.1 FIPS and NDcPP – <37.272`

Vulnerabilidad de restricción inapropiada de operaciones dentro de los límites de un búfer de memoria en Citrix NetScaler ADC y NetScaler Gateway.

Impacto: La explotación de esta vulnerabilidad podría provocar una denegación de servicio (DoS) en los dispositivos afectados.

> **Acción a seguir:** Actualizar a las versiones 14.1 – >=72.61; 13.1 – >=63.18; 14.1 FIPS – >=72.61; 13.1 FIPS and NDcPP – >=37.272. Plazo: 2026-08-29.

Ampliar información: NVD — CVE-2026-8452 CISA KEV

Alta · CVSS 8.1 EXPLOTACIÓN ACTIVA CVE-2021-23758

Ajax.NET Professional Deserialization of Untrusted Data Vulnerability

Ajax.NET Professional Ajax.NET Professional · · Versiones afectadas: `<unspecified`

Vulnerabilidad de deserialización de datos no confiables en Ajax.NET Professional (AjaxPro).

Impacto: Permite la ejecución remota de código a través de clases .NET arbitrarias. El producto podría estar al final de su vida útil (EoL) o servicio (EoS).

> **Acción a seguir:** Se recomienda descontinuar el uso del producto o hacer la transición a una alternativa soportada, si aplica. Plazo: 2026-09-09.

Ampliar información: NVD — CVE-2021-23758 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2026-53362

Linux Kernel Unspecified Vulnerability

Linux Kernel · · Versiones afectadas: `773ba4fe9104a64a54d1c00f0fb6ffb95def2b03 – <14200d435af9a9eeb444f529fc2f689a236b7962`

Vulnerabilidad no especificada en el subsistema de red IPv6 del kernel de Linux.

Impacto: Permite la escalada de privilegios en sistemas que usan el kernel de Linux, afectando a distribuciones como Suse y Red Hat.

> **Acción a seguir:** Actualizar el kernel de Linux a versiones posteriores a 14200d435af9a9eeb444f529fc2f689a236b7962. Plazo: 2026-08-30.

Ampliar información: NVD — CVE-2026-53362 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2022-0995

Linux Kernel Out-of-Bounds Write Vulnerability

Linux Kernel · · Versiones afectadas: `kernel 5.17 rc8`

Vulnerabilidad de escritura fuera de límites de memoria en el kernel de Linux.

Impacto: Un usuario local podría obtener acceso privilegiado o causar una denegación de servicio en el sistema.

> **Acción a seguir:** Actualizar el kernel de Linux a versiones superiores a 5.17 rc8. Plazo: 2026-09-09.

Ampliar información: NVD — CVE-2022-0995 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2015-5287

Red Hat Automatic Bug Reporting Tool Privilege Escalation Vulnerability

Red Hat Automatic Bug Reporting Tool · · Versiones afectadas: -

Vulnerabilidad de escalada de privilegios en Red Hat Automatic Bug Reporting Tool (ABRT).

Impacto: Permite a usuarios locales con ciertos permisos obtener privilegios a través de un ataque de symlink en un archivo con un nombre predecible. El producto podría estar EoL/EoS.

> **Acción a seguir:** Se recomienda descontinuar el uso del producto o hacer la transición a una alternativa soportada, si aplica. Plazo: 2026-09-09.

Ampliar información: NVD — CVE-2015-5287 CISA KEV

MALWARE Y CAMPAÑAS

RedC2 4.0 Backdoor (vía paquetes npm maliciosos)

Se han descubierto 14 paquetes npm trojanizados que distribuyen el backdoor RedC2 4.0 en sistemas Linux. Este implante de C2 asistido por IA es capaz de robo de credenciales, vigilancia y otras actividades maliciosas, representando un ataque a la cadena de suministro.

MITRE ATT&CK: `T1566.001 — Software Supply Chain Compromise` `T1071.001 — Application Layer Protocol: Web Protocols` `T1003 — OS Credential Dump` `T1056 — Input Capture`

> **Acción a seguir:** Auditar dependencias de proyectos npm, evitar la instalación de paquetes de fuentes no confiables y monitorear el tráfico de red en busca de comunicaciones C2 inusuales en sistemas Linux.

SPECTRE Malware (empleado por UAT-10147)

El grupo UAT-10147 está empleando inteligencia artificial para optimizar ataques a servidores web Windows y Linux, desplegando el malware SPECTRE. Este malware está diseñado para evadir soluciones EDR, intensificando la amenaza para la infraestructura crítica.

MITRE ATT&CK: `T1027 — Obfuscated Files or Information` `T1562.001 — Impair Defenses: Disable or Modify Tools`

> **Acción a seguir:** Implementar defensas en capas, monitoreo avanzado de endpoints y tráfico de red para detectar anomalías. Fortalecer las configuraciones de seguridad en servidores Windows y Linux y evaluar la efectividad de las soluciones EDR contra técnicas de evasión.

Manic Malware (Android con exfiltración Wi-Fi mesh)

Un nuevo malware Android llamado 'Manic' combina capacidades de robo bancario y espionaje. Utiliza una innovadora técnica de Wi-Fi mesh para exfiltrar datos, incluso de dispositivos offline, a través de otros equipos infectados, aumentando su persistencia y capacidad de evasión.

MITRE ATT&CK: `T1041 — Exfiltration Over C2 Channel` `T1056 — Input Capture` `T1003 — OS Credential Dump`

> **Acción a seguir:** Alertar a usuarios sobre descargas de aplicaciones de fuentes no oficiales, promover la revisión de permisos de aplicaciones y mantener los sistemas operativos móviles actualizados. Monitorear comportamientos inusuales de la red en dispositivos móviles.

Malware Android en Sistemas de Infoentretenimiento Vehicular

Se ha descubierto un nuevo malware Android que infecta sistemas de infoentretenimiento vehicular a través de actualizaciones, creando botnets y facilitando el fraude publicitario. Esta amenaza subraya la creciente superficie de ataque en vehículos conectados.

MITRE ATT&CK: `T1566.001 — Software Supply Chain Compromise` `T1071.001 — Application Layer Protocol: Web Protocols`

> **Acción a seguir:** Revisar la configuración de actualizaciones de software en sistemas de infoentretenimiento vehicular, asegurándose de que provengan únicamente de fuentes oficiales y de confianza. Implementar medidas de seguridad para proteger la cadena de suministro de software.

NOTICIAS DE CIBERSEGURIDAD

Vulnerabilidad Zero-Day en PaperCut NG y MF Explotada Activamente

Se ha alertado sobre una vulnerabilidad zero-day crítica en PaperCut NG y MF que está siendo explotada activamente. Se recomienda a los usuarios y administradores de estos sistemas tomar medidas inmediatas para proteger sus entornos.

Next.js corrige fallas críticas de RCE en AVIF y Windows

El framework Next.js ha lanzado parches para corregir vulnerabilidades críticas de ejecución remota de código (RCE) que afectaban a AVIF y sistemas Windows. Se insta a los desarrolladores a actualizar sus aplicaciones web para protegerse de posibles ataques no autenticados.

Agentes de IA de OpenAI Explotan Zero-Days y Vulneran Hugging Face y Sistemas Internos

OpenAI ha revelado que sus agentes de inteligencia artificial, entrenados para tareas de ciberseguridad, lograron explotar vulnerabilidades zero-day en plataformas como Artifactory y Hugging Face, así como vulnerar sus propios sistemas internos, destacando el potencial de la IA en la ofensiva y defensa cibernética.

WhatsApp Refuerza Seguridad de Cuentas con Múltiples Passkeys y 2FA Avanzado

WhatsApp ha implementado nuevas características de seguridad para sus cuentas, incluyendo el soporte para múltiples passkeys y una verificación de dos pasos más robusta. Estas mejoras buscan fortalecer la protección de los usuarios contra ataques de phishing y acceso no autorizado en dispositivos iOS y Android.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación de parches para las vulnerabilidades críticas de Oracle (CVE-2026-21962), ownCloud (CVE-2023-49105), Zimbra (CVE-2026-73570) y Gitea (CVE-2026-60004) con fecha límite esta semana. Revise los sistemas Citrix NetScaler y Microsoft SQL Server. Para el malware, audite las dependencias npm en entornos Linux, fortalezca la seguridad de servidores Windows y Linux, y eduque a usuarios sobre riesgos de aplicaciones móviles y actualizaciones vehiculares no oficiales. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) está preparado para detectar y responder a estas amenazas.

AVISO: Boletín informativo TLP:CLEAR de Ingeniería Telemática S.A.S. Datos provenientes de CISA KEV, NVD y avisos de fabricante. De carácter informativo; no sustituye un análisis de su entorno.