INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W36 · 31 ago 2026 – 6 sep 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta semana, el panorama de ciberseguridad destaca varias vulnerabilidades críticas con explotación activa. Las organizaciones deben prestar atención urgente a fallas en SonicWall SMA1000 Appliances, JFrog Artifactory y Kestra OSS, que requieren parcheado inmediato antes del 5 de septiembre. Google Chrome también ha corregido una vulnerabilidad zero-day en su motor V8, lo que subraya la importancia de mantener los navegadores actualizados. En cuanto a las amenazas persistentes, se observa el uso innovador de Node.js por atacantes para distribuir malware, nuevas variantes como TerminalFix que emplean CAPTCHAs falsos, la integración de IA por parte del grupo de ransomware Aurora para optimizar sus ataques y la propagación del troyano bancario StreamRat Android a través de Meta Ads. La pronta aplicación de parches y un monitoreo activo son esenciales para proteger la infraestructura y los datos.

5 Crítica · 3 Alta

Publicado 7 sep 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)

5	3	0	0
Crítica	Alta	Media	Baja

8 vulnerabilidades con explotación activa confirmada · 4 campaña(s) de malware · 6 noticia(s)

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-83548

SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability

SonicWall SMA1000 Appliances · · Versiones afectadas: -

Esta vulnerabilidad de Server-Side Request Forgery (SSRF) en los dispositivos SonicWall SMA1000 permite a un atacante remoto no autenticado obtener acceso no autorizado a funcionalidades sensibles y realizar operaciones no autorizadas.

Impacto: Acceso no autorizado a funciones críticas, posible manipulación de operaciones internas del sistema.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad disponibles proporcionadas por SonicWall antes del 5 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-83548 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-49869

Kestra OSS OS Command Injection Vulnerability

Kestra Kestra OSS · · Versiones afectadas: `< 1.0.45; ⩾ 1.1.0, < 1.3.21`

Una inyección de comandos del sistema operativo en Kestra OSS permite a un atacante remoto no autenticado crear y ejecutar flujos de trabajo arbitrarios sin necesidad de credenciales.

Impacto: Ejecución remota de comandos arbitrarios, control total sobre los flujos de trabajo de Kestra OSS.

> **Acción a seguir:** Actualizar Kestra OSS a la versión 1.0.45 o superior, y a las versiones 1.3.21 o superior para las ramas >= 1.1.0, antes del 5 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-49869 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-82329

JFrog Artifactory Improper Authentication Vulnerability

JFrog Artifactory · · Versiones afectadas: `<7.111.21; 7.117.0 - <7.117.28; 7.125.0 - <7.125.20; 7.133.0 - <7.133.29; 7.146.0 - <7.146.38`

Esta vulnerabilidad de autenticación impropia en JFrog Artifactory, bajo la configuración predeterminada, permite a un atacante no autenticado con acceso a la red obtener privilegios administrativos.

Impacto: Compromiso total del sistema, acceso administrativo no autorizado.

> **Acción a seguir:** Actualizar JFrog Artifactory a las versiones 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38 o superior, según la rama utilizada, antes del 5 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-82329 CISA KEV

Crítica · CVSS 9.4 EXPLOTACIÓN ACTIVA CVE-2026-82078

PaperCut NG/MF Unsafe Reflection Vulnerability

PaperCut NG/MF · · Versiones afectadas: <24.1.10, 25.0.13, 26.0.5

Una vulnerabilidad de reflexión insegura en PaperCut NG/MF permite a un atacante manipular parámetros de configuración del sistema y ejecutar bytecode Java arbitrario con los privilegios del proceso del servidor PaperCut.

Impacto: Ejecución de código arbitrario, manipulación de la configuración del sistema, posible escalada de privilegios.

> **Acción a seguir:** Actualizar PaperCut NG/MF a las versiones 24.1.10, 25.0.13, 26.0.5 o superiores antes del 14 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-82078 CISA KEV

Crítica · CVSS 9.3 EXPLOTACIÓN ACTIVA CVE-2026-9586

Sangoma Switchvox SQL Injection Vulnerability

Sangoma Switchvox · · Versiones afectadas: 8.3 (104997) – <8.4.0.2

Una vulnerabilidad de inyección SQL en Sangoma Switchvox permite a un atacante remoto no autenticado ejecutar sentencias SQL arbitrarias contra la base de datos PostgreSQL, incluyendo operaciones de base de datos y ejecución remota de código.

Impacto: Acceso y manipulación de la base de datos, ejecución remota de código, posible compromiso del sistema.

> **Acción a seguir:** Actualizar Sangoma Switchvox a la versión 8.4.0.2 o superior antes del 5 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-9586 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2026-85046

Google Chromium V8 Type Confusion Vulnerability

Google Chromium V8 · · Versiones afectadas: 152.0.7977.82 – <152.0.7977.82

Esta vulnerabilidad de confusión de tipos en Google Chromium V8 permite a un atacante remoto ejecutar código arbitrario dentro del sandbox del navegador a través de una página HTML manipulada. Afecta a múltiples navegadores que utilizan Chromium, incluyendo Google Chrome y Microsoft Edge.

Impacto: Ejecución de código arbitrario en el contexto del navegador, posible evasión del sandbox y compromiso del sistema.

> **Acción a seguir:** Actualizar Google Chrome y otros navegadores basados en Chromium a la versión 152.0.7977.82 o superior antes del 18 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-85046 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2026-59822

BerriAI LiteLLM Improper Authentication Vulnerability

BerriAI LiteLLM · · Versiones afectadas: < 1.84.0

Una vulnerabilidad de autenticación impropia en el endpoint HTTP MCP Streamable de BerriAI LiteLLM permite a un atacante no autenticado establecer una sesión MCP autenticada utilizando un token Bearer arbitrario.

Impacto: Bypass de autenticación, acceso no autorizado a recursos protegidos.

> **Acción a seguir:** Actualizar BerriAI LiteLLM a la versión 1.84.0 o superior antes del 16 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-59822 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2026-83549

SonicWall SMA1000 Appliances OS Command Injection Vulnerability

SonicWall SMA1000 Appliances · · Versiones afectadas: -

Esta vulnerabilidad de inyección de comandos del sistema operativo en los dispositivos SonicWall SMA1000 permite a un atacante remoto autenticado como administrador ejecutar comandos OS arbitrarios, lo que resulta en ejecución remota de código.

Impacto: Ejecución remota de código con privilegios de administrador, compromiso total del sistema.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad disponibles proporcionadas por SonicWall antes del 5 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-83549 CISA KEV

MALWARE Y CAMPAÑAS

Node.js como herramienta de distribución de malware (AdaptixC2, C2Looper)

Ciberatacantes están utilizando Node.js, una plataforma de ejecución JavaScript legítima, como un vector para distribuir malware como AdaptixC2 y C2Looper. Esta táctica les permite evadir las defensas tradicionales al abusar de una herramienta de desarrollo conocida para ejecutar payloads maliciosos y establecer canales persistentes de comando y control en redes corporativas.

MITRE ATT&CK: `T1059.007 — Command and Scripting Interpreter: JavaScript/JScript` `T1203 — Exploitation for Client Execution` `T1071.001 — Application Layer Protocol: Web Protocols`

> **Acción a seguir:** Implementar controles de aplicación para restringir la ejecución de Node.js en sistemas donde no sea estrictamente necesario. Monitorear la actividad de red en busca de comunicaciones salientes sospechosas y la ejecución de scripts ofuscados o anómalos.

TerminalFix

TerminalFix es una variante de malware que engaña a los usuarios mediante CAPTCHAs falsos para ejecutar comandos PowerShell maliciosos. Una vez activado, establece un túnel inverso, permitiendo a los atacantes mantener el control de la red comprometida y acceder a recursos internos.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1059.001 — Command and Scripting Interpreter: PowerShell` `T1572 — Protocol Tunneling`

> **Acción a seguir:** Educar a los usuarios sobre los riesgos de los CAPTCHAs y enlaces sospechosos. Implementar soluciones EDR y antivirus con análisis de comportamiento para detectar la ejecución de scripts anómalos de PowerShell y actividades de tunelización.

Ransomware Aurora con integración de IA

El grupo de ransomware Aurora ha sido detectado utilizando asistentes de Inteligencia Artificial, como Cursor AI, para planificar y ejecutar sus ciberataques. Esta integración de IA permite una mayor sofisticación en la evasión de defensas, la creación de código malicioso y el reconocimiento de la infraestructura de la víctima, haciendo sus ataques más eficientes y difíciles de detectar.

MITRE ATT&CK: `T1486 — Data Encrypted for Impact` `T1059 — Command and Scripting Interpreter` `T1584 — Compromise Infrastructure`

> **Acción a seguir:** Implementar soluciones avanzadas de seguridad que incluyan detección basada en IA para patrones de ataque emergentes. Reforzar la segmentación de red, las copias de seguridad inmutables y la formación del personal en la identificación de tácticas de ingeniería social.

Troyano StreamRat Android

El troyano bancario StreamRat para Android se está propagando activamente a través de anuncios maliciosos en plataformas como Meta Ads (Facebook, Instagram, TikTok). Este malware busca obtener control total sobre los dispositivos Android infectados con el objetivo de robar credenciales bancarias y otra información sensible de los usuarios.

MITRE ATT&CK: `T1566.002 — Phishing: Spearphishing Link` `T1413 — Drive-by Compromise` `T1555 — Credentials from Password Stores`

> **Acción a seguir:** Aconsejar a los empleados sobre los riesgos de descargar aplicaciones de fuentes no verificadas y hacer clic en anuncios sospechosos en redes sociales. Utilizar soluciones EDR/MDR para dispositivos móviles con capacidades de detección y mitigación de amenazas.

NOTICIAS DE CIBERSEGURIDAD

IA Claude Genera Exploit RCE en PLCs WAGO, Impactando la Ciberseguridad OT Industrial

Investigadores lograron portar un exploit de ejecución remota de código (RCE) en PLCs WAGO (CVE-2021-31886) utilizando la inteligencia artificial Claude. Este desarrollo subraya la creciente capacidad de las herramientas de IA para facilitar la creación de exploits y la evolución de las amenazas en el ámbito de la ciberseguridad industrial y de OT.

Alerta Crítica: Explotación Activa de Vulnerabilidades RCE en Plugins Super Forms y Elementor Pro de WordPress

Se ha detectado la explotación activa de vulnerabilidades de ejecución remota de código (RCE) en plugins populares de WordPress como Super Forms y Elementor Pro. Los atacantes están aprovechando estas fallas para inyectar web shells y obtener control total de los sitios web, lo que requiere una acción inmediata mediante parches y la implementación de Web Application Firewalls (WAF).

Vulnerabilidades Críticas en Plugins y Temas de WordPress: Riesgo de Toma de Control y RCE

Múltiples fallas críticas han sido identificadas en plugins y temas populares de WordPress, incluyendo WPMU DEV Dashboard, Avada, TranslatePress, Pods y GiveWP. Estas vulnerabilidades exponen los sitios a ejecución remota de código (RCE), bypass de autenticación y toma de control completa, destacando la necesidad de mantener todos los componentes de WordPress actualizados y seguros.

Cisco Alerta: Fallas Críticas de RCE en Nexus 9000 y Múltiples CVEs de IOS XR Requieren Parches Urgentes

Cisco ha emitido una alerta sobre una vulnerabilidad crítica de ejecución remota de código (RCE) no autenticada (CVE-2026-20212) en sus dispositivos Nexus 9000, junto con múltiples CVEs de alta gravedad en Cisco IOS XR. Es imperativo que las organizaciones actualicen sus dispositivos para mitigar estos riesgos que podrían comprometer seriamente la infraestructura de red.

Explotación Activa de Vulnerabilidades Críticas en Langflow y Ruby on Rails para Robo de Credenciales

Se ha detectado la explotación activa de vulnerabilidades críticas (CVE-2026-0768, CVE-2026-66066) en plataformas como Langflow y Ruby on Rails. Estas explotaciones están siendo utilizadas para la ejecución remota de código, el robo de credenciales y el establecimiento de canales de comando y control, afectando la seguridad de las aplicaciones web que utilizan estas tecnologías.

Vulnerabilidades Críticas en Next.js Permiten Ejecución Remota de Código (RCE) sin Autenticación

Next.js ha publicado parches para corregir dos vulnerabilidades críticas (CVE-2026-75604, GHSA-2xp9-vwfh-vxw4) que permiten la ejecución remota de código (RCE) sin autenticación. Estas fallas se relacionan con el procesamiento de archivos AVIF y una vulnerabilidad de path traversal en sistemas Windows, poniendo en riesgo las aplicaciones desarrolladas con Next.js.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación inmediata de los parches para las vulnerabilidades críticas de SonicWall SMA1000 (CVE-2026-83548, CVE-2026-83549), Kestra OSS (CVE-2026-49869), JFrog Artifactory (CVE-2026-82329) y Sangoma Switchvox (CVE-2026-9586), ya que sus plazos de CISA vencen el 5 de septiembre de 2026. Actualice urgentemente Google Chrome (CVE-2026-85046) y PaperCut NG/MF (CVE-2026-82078) antes de sus respectivos plazos en septiembre. Mantenga una vigilancia estricta sobre la actividad de red y el comportamiento de las aplicaciones para detectar indicadores de compromiso relacionados con las campañas de malware Node.js, TerminalFix, Aurora ransomware (con IA) y el troyano StreamRat Android. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) está preparado para detectar y mitigar estas amenazas.