INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W25 · 15 jun 2026 – 21 jun 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta edición del Boletín Semanal de Ciberseguridad destaca la presencia de cuatro vulnerabilidades con explotación activa, según CISA, incluyendo dos de severidad Crítica en Widget Factory Joomla Content Editor y Splunk Enterprise, y una Alta en LiteSpeed cPanel Plugin, todas con plazos de remediación inminentes. Adicionalmente, se advierte sobre la sofisticación creciente de amenazas, como el uso del backdoor Backdoor.Turn por el grupo DragonForce para ocultar tráfico de Comando y Control (C2) mediante el abuso de Microsoft Teams en ataques de ransomware. También se analiza el surgimiento de campañas de smishing y phishing potenciadas por IA, ilustrado por la demanda de Google contra una red que utilizaba Gemini. Es crucial priorizar la aplicación de parches y fortalecer el monitoreo de red para mitigar estos riesgos.

2 Crítica | 1 Alta | 1 Media

Publicado 22 jun 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)

2	1	1	0
Crítica	Alta	Media	Baja

4 vulnerabilidades con explotación activa confirmada · 1 campaña(s) de malware · 1 noticia(s)

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-48907

Vulnerabilidad de Control de Acceso Impropio en Widget Factory Joomla Content Editor

Widget Factory Joomla Content Editor · CWE-284: Improper Access Control · Versiones afectadas: `1.0.0-2.9.99.4`

Widget Factory Joomla Content Editor contiene una vulnerabilidad de control de acceso impropio que podría permitir la carga y ejecución de código PHP.

Impacto: Un atacante no autenticado podría explotar esta vulnerabilidad para crear nuevos perfiles de editor, cargar y ejecutar código PHP malicioso en el servidor, lo que llevaría a una completa toma de control del sistema (RCE).

> **Acción a seguir:** Se recomienda encarecidamente actualizar Widget Factory Joomla Content Editor a una versión superior a la 2.9.99.4 antes del 19 de junio de 2026.

Ampliar información: NVD — CVE-2026-48907 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-20253

Vulnerabilidad de Autenticación Faltante para Función Crítica en Splunk Enterprise

Splunk Enterprise · CWE-306: Missing Authentication for Critical Function · Versiones afectadas: `10.2 - <10.2.4; 10.0 - <10.0.7`

Splunk Enterprise contiene una vulnerabilidad de falta de autenticación para una función crítica, la cual podría permitir a un usuario no autenticado crear o truncar archivos arbitrarios a través de un endpoint del servicio PostgreSQL sidecar.

Impacto: Un atacante no autenticado podría manipular o causar una denegación de servicio de datos críticos al crear o truncar archivos arbitrarios, lo que podría afectar la disponibilidad e integridad del sistema.

> **Acción a seguir:** Actualizar Splunk Enterprise a la versión 10.2.4 o superior (para la rama 10.2) o a la versión 10.0.7 o superior (para la rama 10.0) antes del 21 de junio de 2026.

Ampliar información: NVD — CVE-2026-20253 CISA KEV

Alta · CVSS 8.5 EXPLOTACIÓN ACTIVA CVE-2026-54420

Vulnerabilidad de Seguimiento de Enlaces Simbólicos (Symlink) en LiteSpeed cPanel Plugin

LiteSpeed cPanel Plugin · CWE-59: Improper Link Resolution Before File Access ('Link Following') · Versiones afectadas: `2.3 - <2.4.8`

El plugin LiteSpeed cPanel contiene una vulnerabilidad de seguimiento de enlaces simbólicos (Symlink).

Impacto: Un usuario con acceso FTP o shell web en un servidor de hosting compartido que ejecute CloudLinux/CageFS podría explotar esta vulnerabilidad para obtener acceso no autorizado a archivos y directorios fuera de su directorio raíz, lo que podría conducir a la escalada de privilegios o el acceso a información sensible.

> **Acción a seguir:** Actualizar el plugin LiteSpeed cPanel a la versión 2.4.8 o superior antes del 18 de junio de 2026.

Ampliar información: NVD — CVE-2026-54420 CISA KEV

Media · CVSS 6.5 EXPLOTACIÓN ACTIVA CVE-2026-20262

Vulnerabilidad de Recorrido de Directorio o Ruta en Cisco Catalyst SD-WAN Manager

Cisco Catalyst SD-WAN Manager · CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') · Versiones afectadas: `20.1.12; 19.2.1; 18.4.4; 18.4.5; 20.1.1.1`

Cisco Catalyst SD-WAN Manager contiene una vulnerabilidad de recorrido de directorio o ruta.

Impacto: Un atacante remoto autenticado podría crear o sobrescribir archivos arbitrarios en el sistema de archivos del sistema afectado, lo que podría comprometer la integridad del sistema o facilitar otros ataques.

> **Acción a seguir:** Actualizar Cisco Catalyst SD-WAN Manager a una versión superior a 20.1.12, 19.2.1, 18.4.4, 18.4.5 o 20.1.1.1. La fecha límite de CISA para esta remediación es el 29 de junio de 2026.

Ampliar información: NVD — CVE-2026-20262 CISA KEV

MALWARE Y CAMPAÑAS

DragonForce (Backdoor.Turn)

El grupo de ransomware DragonForce está utilizando el backdoor Backdoor.Turn y abusando de los retransmisores de Microsoft Teams para ofuscar y ocultar su tráfico de Comando y Control (C2), lo que dificulta su detección en los ataques de ransomware.

MITRE ATT&CK: `T1486 — Data Encrypted for Impact` `T1071.001 — Application Layer Protocol: Web Protocols` `T1573 — Encrypted Channel`

> **Acción a seguir:** Implementar monitoreo de tráfico de red para detectar comunicaciones anómalas, especialmente aquellas que abusan de servicios legítimos como Microsoft Teams para C2. Reforzar la seguridad de endpoints y la detección de backdoors.

NOTICIAS DE CIBERSEGURIDAD

Google Demanda Red de Smishing con IA Gemini: La Evolución del Phishing

Google ha presentado una demanda contra una red criminal china que explotó la inteligencia artificial Gemini para orquestar campañas de smishing (phishing por SMS) y phishing altamente sofisticadas, marcando una nueva y preocupante fase en la evolución de estas amenazas.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorizar la aplicación de parches para las vulnerabilidades críticas con explotación activa, especialmente CVE-2026-54420 (LiteSpeed cPanel Plugin) y CVE-2026-48907 (Widget Factory Joomla Content Editor) antes de sus fechas límite del 18 y 19 de junio, respectivamente, seguidas de CVE-2026-20253 (Splunk Enterprise) antes del 21 de junio. Mantener una vigilancia constante sobre el tráfico de red para identificar patrones de Comando y Control (C2) que puedan estar utilizando servicios legítimos como Microsoft Teams, como se observa en los ataques de DragonForce. Para un acompañamiento continuo, nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está disponible para proteger su infraestructura contra estas y otras amenazas emergentes.