INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W30 · 20 jul 2026 – 26 jul 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta semana, el panorama de ciberseguridad se ha visto marcado por la explotación activa de múltiples vulnerabilidades críticas, demandando una acción inmediata. Destacan fallas de ejecución remota de código (RCE) en Microsoft SharePoint, Langflow, WordPress Core y Check Point SmartConsole, todas con plazos de parcheo urgentes. Además, nuevas campañas de ransomware como Qilin y ENCFORGE están aprovechando activamente estas debilidades. Se observan también sofisticados kits de phishing como Kratos, la evasión de defensas con malware como HollowGraph, y el descubrimiento de nuevas amenazas como Bit2Watt, capaz de desestabilizar infraestructuras críticas desde la nube, junto con vulnerabilidades zero-day en Redis y NGINX. La consultora Ingeniería Telemática S.A.S. recomienda una revisión exhaustiva de los sistemas y la aplicación prioritaria de las mitigaciones detalladas.

4 Crítica | 1 Alta | 1 Media

Publicado 27 jul 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)

4	1	1	0
Crítica	Alta	Media	Baja

6 vulnerabilidades con explotación activa confirmada · 5 campaña(s) de malware · 4 noticia(s)

VULNERABILIDADES

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-50522

Vulnerabilidad de Deserialización de Datos no Confiables en Microsoft SharePoint

Microsoft SharePoint · CWE-502: Deserialization of Untrusted Data · Versiones afectadas: `16.0.0 - <16.0.5561.1001; 16.0.0 - <16.0.10417.20175; 16.0.0 - <16.0.19725.20434`

Microsoft SharePoint contiene una vulnerabilidad de deserialización de datos no confiables que podría permitir a un atacante no autorizado ejecutar código de forma remota a través de la red.

Impacto: Un atacante no autenticado puede lograr la ejecución remota de código arbitrario en el servidor afectado, comprometiendo gravemente la confidencialidad, integridad y disponibilidad de los datos y servicios de SharePoint.

> **Acción a seguir:** Es crucial actualizar inmediatamente Microsoft SharePoint a las versiones 16.0.5561.1001, 16.0.10417.20175 o 16.0.19725.20434 o superiores, según la rama de versión utilizada. CISA exige aplicar este parche antes del 25 de julio de 2026.

Ampliar información: NVD — CVE-2026-50522 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-0770

Vulnerabilidad de Inclusión de Funcionalidad desde Esfera de Control No Confiable en Langflow

Langflow Langflow · CWE-829: Inclusion of Functionality from Untrusted Control Sphere · Versiones afectadas: `1.4.2`

Langflow contiene una vulnerabilidad que permite la inclusión de funcionalidad desde una esfera de control no confiable, lo que podría habilitar a atacantes remotos para ejecutar código arbitrario.

Impacto: Atacantes remotos pueden ejecutar código arbitrario con los privilegios de la aplicación, obteniendo control total sobre las instalaciones de Langflow. Esto puede conducir a la manipulación de flujos de trabajo de IA, exfiltración de datos o compromiso del sistema subyacente.

> **Acción a seguir:** Es imperativo actualizar Langflow a una versión parcheada que resuelva esta vulnerabilidad. La versión 1.4.2 es vulnerable. CISA exige aplicar este parche antes del 24 de julio de 2026.

Ampliar información: NVD — CVE-2026-0770 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-63030

Vulnerabilidad de Conflicto de Interpretación en WordPress Core

WordPress Core · CWE-436: Interpretation Conflict · Versiones afectadas: `6.9.0 - <6.9.5; 7.0.0 - <7.0.2`

WordPress Core presenta una vulnerabilidad de conflicto de interpretación que, en combinación con CVE-2026-60137, puede permitir la inyección SQL y la ejecución remota de código.

Impacto: Un atacante no autenticado podría explotar esta vulnerabilidad para ejecutar código arbitrario de forma remota en instalaciones predeterminadas de WordPress, resultando en un compromiso completo del sitio web y su base de datos.

> **Acción a seguir:** Actualizar WordPress Core a la versión 6.9.5 o superior para la rama 6.9.x, o a la versión 7.0.2 o superior para la rama 7.0.x. CISA exige aplicar este parche antes del 24 de julio de 2026.

Ampliar información: NVD — CVE-2026-63030 CISA KEV

Crítica · CVSS 9.1 EXPLOTACIÓN ACTIVA CVE-2026-16232

Vulnerabilidad de Autenticación Inapropiada en Check Point SmartConsole

Check Point SmartConsole · CWE-287: Improper Authentication · Versiones afectadas: `R82 with Jumbo Hotfix Take 118 or below`

Check Point SmartConsole contiene una vulnerabilidad de autenticación inapropiada que podría permitir a un atacante remoto no autenticado obtener un token de inicio de sesión de la aplicación y autenticarse con privilegios de administrador.

Impacto: Un atacante remoto puede obtener control administrativo completo sobre Check Point SmartConsole, permitiéndole manipular la configuración de seguridad, políticas y dispositivos de red gestionados.

> **Acción a seguir:** Aplicar el Jumbo Hotfix Take 119 o superior para la versión R82 de Check Point SmartConsole. CISA exige aplicar este parche antes del 25 de julio de 2026.

Ampliar información: NVD — CVE-2026-16232 CISA KEV

Alta · CVSS 8.1 EXPLOTACIÓN ACTIVA CVE-2021-27137

Vulnerabilidad de Desbordamiento de Búfer Basado en Pila en DD-WRT

DD-WRT DD-WRT · CWE-121: Stack-based Buffer Overflow · Versiones afectadas: <45724

DD-WRT es susceptible a una vulnerabilidad de desbordamiento de búfer basado en pila que puede ser explotada por un atacante no autenticado a través de la funcionalidad UPnP.

Impacto: Un atacante no autenticado puede desbordar un búfer interno del UPnP, lo que puede desencadenar la ejecución de código arbitrario y tomar el control del dispositivo DD-WRT.

> **Acción a seguir:** Actualizar DD-WRT a la versión 45724 o superior. CISA exige aplicar este parche antes del 24 de julio de 2026.

Ampliar información: NVD — CVE-2021-27137 CISA KEV

Media · CVSS 5.9 EXPLOTACIÓN ACTIVA CVE-2026-60137

Vulnerabilidad de Inyección SQL en WordPress Core

WordPress Core · CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') · Versiones afectadas: `6.8.0 - <6.8.6; 6.9.0 - <6.9.5; 7.0.0 - <7.0.2`

WordPress Core contiene una vulnerabilidad de inyección SQL que se produce cuando un plugin o tema pasa entrada no confiable a un parámetro específico de la base de datos. Esta vulnerabilidad puede ser encadenada con CVE-2026-63030 para lograr RCE.

Impacto: Un atacante no autenticado puede manipular consultas SQL para acceder, modificar o eliminar datos de la base de datos. Cuando se encadena con CVE-2026-63030, puede llevar a la ejecución remota de código.

> **Acción a seguir:** Actualizar WordPress Core a la versión 6.8.6 o superior para la rama 6.8.x, 6.9.5 o superior para la rama 6.9.x, o 7.0.2 o superior para la rama 7.0.x. CISA exige aplicar este parche antes del 4 de agosto de 2026.

Ampliar información: NVD — CVE-2026-60137 CISA KEV

MALWARE Y CAMPAÑAS

Ransomware Qilin

La banda de ransomware Qilin está explotando activamente la vulnerabilidad CVE-2026-0257 en PAN-OS de Palo Alto Networks. Esta explotación permite el bypass de autenticación, facilitando el acceso inicial a las redes corporativas y la posterior implementación del ransomware para cifrar datos.

MITRE ATT&CK: `T1190 — Exploit Public-Facing Application` `T1078 — Valid Accounts` `T1486 — Data Encrypted for Impact`

> **Acción a seguir:** Los administradores de sistemas deben verificar urgentemente la actualización de sus dispositivos PAN-OS y aplicar los parches correspondientes para CVE-2026-0257. Se recomienda implementar una segmentación de red robusta y un monitoreo continuo para detectar cualquier actividad anómala o intento de movimiento lateral.

Ransomware ENCFORGE

El grupo JADEPUFFER ha desplegado el ransomware ENCFORGE, el cual se enfoca en explotar vulnerabilidades de ejecución remota de código (RCE) en Langflow para cifrar archivos de modelos y datos de entrenamiento de inteligencia artificial, interrumpiendo gravemente las operaciones de sistemas de IA.

MITRE ATT&CK: `T1190 — Exploit Public-Facing Application` `T1486 — Data Encrypted for Impact` `T1071 — Application Layer Protocol`

> **Acción a seguir:** Es fundamental proteger los sistemas Langflow aplicando de inmediato los parches disponibles para cualquier vulnerabilidad RCE conocida. Se debe asegurar la implementación de copias de seguridad de los modelos y datos de IA, además de segmentar las redes para limitar la propagación del ransomware.

Campaña de Malware WebDAV con Toolkit de Phishing con IA

Se ha descubierto una campaña de malware WebDAV que utiliza un sofisticado toolkit de phishing impulsado por inteligencia artificial. Esta campaña, que afectó a usuarios en México, se apoya en la explotación de la CVE-2025-33053 para comprometer sistemas.

MITRE ATT&CK: `T1566.002 — Spearphishing Link` `T1566.001 — Spearphishing Attachment` `T1071 — Application Layer Protocol`

> **Acción a seguir:** Es vital capacitar a los usuarios sobre cómo identificar correos electrónicos de phishing, especialmente aquellos que utilizan técnicas avanzadas con IA. Implementar autenticación multifactor (MFA) robusta y soluciones de seguridad de endpoints capaces de detectar malware WebDAV y la explotación de CVEs conocidos.

Kit de Phishing Kratos

Kratos, un sofisticado kit de phishing diseñado para robar sesiones de Microsoft 365 y eludir la autenticación multifactor (MFA), ha sido desmantelado en una operación global. Este kit permitía a los atacantes acceder a cuentas incluso con MFA activado.

MITRE ATT&CK: `T1566.001 — Spearphishing Attachment` `T1566.002 — Spearphishing Link` `T1550.002 — Steal Web Session Cookie` `T1078 — Valid Accounts`

> **Acción a seguir:** Aunque Kratos ha sido desmantelado, las organizaciones deben fortalecer sus políticas de MFA y educar continuamente a los usuarios sobre la identificación de correos electrónicos de phishing. Implementar defensas sólidas contra ataques de suplantación de identidad y monitorear anomalías en el inicio de sesión es fundamental.

Malware HollowGraph

HollowGraph es un malware de espionaje que utiliza eventos de calendario de Microsoft 365 con fechas lejanas (como el año 2050) para establecer canales de Comando y Control (C2) y exfiltrar datos. Este método innovador permite al malware evadir las defensas de seguridad tradicionales.

MITRE ATT&CK: `T1071.004 — Application Layer Protocol: DNS` `T1071.001 — Application Layer Protocol: HTTP/S` `T1041 — Exfiltration Over C2 Channel`

> **Acción a seguir:** Se recomienda un monitoreo riguroso de actividades inusuales en calendarios y otros servicios de Microsoft 365. La implementación de soluciones EDR/XDR es clave para detectar comportamientos anómalos y exfiltración de datos, incluso a través de canales poco convencionales como eventos de calendario.

NOTICIAS DE CIBERSEGURIDAD

Alerta de Zero-Days Críticos en Redis Permiten RCE

Se han descubierto fallas zero-day críticas en varias versiones de Redis (6.2.22, 7.4.9, 8.6.4, 8.8.0) que permiten la ejecución remota de código (RCE). Estas vulnerabilidades, aún sin parche oficial, representan un riesgo significativo para los sistemas que utilizan Redis como base de datos en memoria.

Bit2Watt: Nuevo Ataque para Desestabilizar Redes Eléctricas desde la Nube

Investigadores han revelado 'Bit2Watt', un método de ataque innovador que permitiría a inquilinos maliciosos de servicios de computación en la nube perturbar y potencialmente desestabilizar redes eléctricas nacionales, utilizando las cargas de trabajo de GPU para manipular la demanda de energía.

Falla en Azure DevOps MCP Permite Secuestro de IA con Comentarios Ocultos

Una vulnerabilidad crítica descubierta en Azure DevOps MCP (Micro-Frontend Control Plane) permite a atacantes insertar comentarios HTML invisibles. Estos comentarios pueden ser utilizados para secuestrar los agentes de IA de revisión de código y exfiltrar datos sensibles de manera encubierta, eludiendo las detecciones estándar.

Alerta Crítica en NGINX: CVE-2026-42533 permite DoS y RCE

Una vulnerabilidad de desbordamiento de búfer de alta criticidad (CVE-2026-42533) ha sido descubierta en NGINX, afectando a versiones lanzadas desde 2011. Esta falla puede ser explotada para causar ataques de Denegación de Servicio (DoS) y, en ciertos escenarios, la ejecución remota de código (RCE), comprometiendo la disponibilidad y seguridad de los servidores.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación inmediata de parches para las vulnerabilidades activamente explotadas de Microsoft SharePoint (CVE-2026-50522), Langflow (CVE-2026-0770), WordPress Core (CVE-2026-63030) y Check Point SmartConsole (CVE-2026-16232) antes de sus respectivos plazos CISA (24 o 25 de julio de 2026). Revise y refuerce la seguridad de dispositivos PAN-OS contra el Ransomware Qilin y sistemas Langflow contra ENCFORGE. Mantenga la concientización sobre técnicas de phishing con IA, y monitoree los sistemas de Microsoft 365 para detectar actividades anómalas como las del malware HollowGraph. Nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a estas amenazas para proteger proactivamente sus activos.