INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W27 · 29 jun 2026 – 5 jul 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta semana, el Boletín de Ciberseguridad de Ingeniería Telemática S.A.S. destaca dos vulnerabilidades bajo explotación activa identificadas por CISA que exigen atención inmediata: un bypass de autenticación crítico (CVSS 9.5) en SimpleHelp, plataforma de soporte remoto, que permite a un atacante no autenticado suplantar la identidad de usuarios cuando está configurada la autenticación OIDC; y una deserialización de datos no confiables en Microsoft SharePoint Server (CVSS 8.8) que habilita la ejecución remota de código. Ambas tienen plazos de remediación inminentes o vencidos según CISA. En el panorama de amenazas, observamos la creciente sofisticación del malware, incluyendo campañas de robo de credenciales como FortiBleed dirigida a FortiGate —ahora vinculada al ransomware INC— y extensiones maliciosas de Edge, así como el surgimiento de amenazas impulsadas por Inteligencia Artificial, como el agente ransomware JADEPUFFER, el ransomware de navegador basado en IA y la técnica de suplantación 'Phantom Squatting'. Se recomienda priorizar el parcheo y fortalecer el monitoreo de endpoints y red para mitigar estos riesgos.

1 Crítica · 1 Alta

Publicado 6 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)

1	1	0	0
Crítica	Alta	Media	Baja

2 vulnerabilidades con explotación activa confirmada · 8 campaña(s) de malware · 3 noticia(s)

VULNERABILIDADES

Crítica · CVSS 9.5 EXPLOTACIÓN ACTIVA CVE-2026-48558

Vulnerabilidad de Bypass de Autenticación en SimpleHelp

SimpleHelp SimpleHelp · CWE-287 · Versiones afectadas: `5.5.0 – <5.5.16; 6.0 – <6.0 RC2`

SimpleHelp presenta una vulnerabilidad de bypass de autenticación en su flujo de autenticación OIDC. Los tokens de identidad enviados durante el inicio de sesión son aceptados sin verificar su firma criptográfica, lo que permite a un atacante remoto no autenticado eludir la autenticación.

Impacto: Acceso no autorizado al sistema SimpleHelp, lo que puede llevar al despliegue de malware como TaskWeaver y Djinn Stealer para el robo de credenciales y otros activos. Los atacantes pueden tomar el control de las sesiones y la información gestionada.

> **Acción a seguir:** Actualice SimpleHelp a la versión 5.5.16 o posterior, o a la versión 6.0 RC2 o posterior. El plazo de CISA para su remediación es el 2 de julio de 2026.

Ampliar información: NVD — CVE-2026-48558 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2026-45659

Vulnerabilidad de Deserialización de Datos no Confiables en Microsoft SharePoint Server

Microsoft SharePoint Server · CWE-502 · Versiones afectadas: `16.0.0 – <16.0.5552.1002; 16.0.0 – <16.0.10417.20128; 16.0.0 – <16.0.19725.20280`

Microsoft SharePoint Server contiene una vulnerabilidad de deserialización de datos no confiables que permite a un atacante autorizado ejecutar código a través de la red.

Impacto: Ejecución remota de código (RCE) con privilegios de un atacante autorizado, lo que puede llevar al compromiso del servidor.

> **Acción a seguir:** Aplique las actualizaciones de seguridad de Microsoft para SharePoint Server a las versiones 16.0.5552.1002, 16.0.10417.20128, 16.0.19725.20280 o posteriores. El plazo de CISA para su remediación es el 4 de julio de 2026.

Ampliar información: NVD — CVE-2026-45659 CISA KEV

MALWARE Y CAMPAÑAS

StegoAd (Extensiones Maliciosas de Microsoft Edge)

Microsoft desactivó 119 extensiones maliciosas de Edge que ocultaban malware en imágenes (esteganografía) para robar credenciales y realizar fraude publicitario, afectando a millones de usuarios. Estas extensiones se hacían pasar por herramientas legítimas para engañar a los usuarios.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1059 — Command and Scripting Interpreter` `T1552.001 — Credential Acquisition: Credentials In Files` `T1189 — Drive-by Compromise`

> **Acción a seguir:** Revise y elimine cualquier extensión de navegador sospechosa. Habilite la autenticación multifactor (MFA) para proteger las cuentas de usuario y eduque a los usuarios sobre los riesgos de descargar extensiones de fuentes no confiables.

JADEPUFFER (Agente de IA Ransomware)

Un agente de Inteligencia Artificial denominado JADEPUFFER ejecutó el primer ataque ransomware 100% automatizado, explotando vulnerabilidades en Langflow y Nacos para cifrar bases de datos. Este evento marca un hito en el uso de IA para la automatización de ciberataques.

MITRE ATT&CK: `T1592 — Gather Victim Host Information` `T1210 — Exploitation of Remote Services` `T1486 — Data Encrypted for Impact` `T1070.004 — Indicator Removal: File Deletion`

> **Acción a seguir:** Mantenga sus sistemas y aplicaciones actualizados con los últimos parches de seguridad, especialmente para plataformas de desarrollo y bases de datos. Implemente un monitoreo de seguridad robusto para detectar actividades anómalas y realice copias de seguridad periódicas de los datos críticos.

Umbrij (ToddyCat APT)

El malware Umbrij, atribuido al grupo APT ToddyCat, explota el protocolo OAuth y la API de Google para comprometer cuentas de Gmail corporativas y robar comunicaciones críticas. Se enfoca en acceder a la información de los buzones de correo sin necesidad de credenciales directas.

MITRE ATT&CK: `T1537 — Transfer Data to Cloud Account` `T1526 — Cloud Service Discovery` `T1136.002 — Create Account: Cloud Account` `T1056.001 — Input Capture: Keylogging`

> **Acción a seguir:** Revise y audite regularmente los permisos de las aplicaciones de terceros que tienen acceso a las cuentas de Google (OAuth). Implemente políticas de menor privilegio y monitoree el acceso a las APIs de Google para detectar comportamientos inusuales.

FortiBleed (Robo de Credenciales de FortiGate)

La campaña 'FortiBleed' está activa, robando credenciales de firewalls FortiGate para luego ser utilizadas en ataques de ransomware por grupos como INC y Lynx. Esta amenaza subraya la importancia de proteger los dispositivos de seguridad de red.

MITRE ATT&CK: `T1552.001 — Credential Acquisition: Credentials In Files` `T1110 — Brute Force` `T1078.002 — Valid Accounts: Domain Accounts` `T1486 — Data Encrypted for Impact`

> **Acción a seguir:** Asegure sus firewalls FortiGate con credenciales robustas, MFA y monitoree los registros de acceso en busca de actividades sospechosas. Aplique las últimas actualizaciones de seguridad de Fortinet y revise las políticas de acceso remoto.

Phantom Squatting (Dominios generados por IA)

Los atacantes están utilizando la técnica 'Phantom Squatting' para registrar dominios falsos generados por IA, que las herramientas de seguridad tradicionales pueden 'alucinar' como legítimos. Estos dominios se usan para lanzar campañas de phishing y malware, evadiendo las defensas convencionales.

MITRE ATT&CK: `T1598.003 — Phishing: Spearphishing Link` `T1071.001 — Application Layer Protocol: Web Protocols` `T1566.001 — Phishing: Spearphishing Attachment`

> **Acción a seguir:** Implemente soluciones avanzadas de detección de amenazas que utilicen análisis de comportamiento y aprendizaje automático para identificar dominios sospechosos. Eduque a los usuarios sobre las tácticas de phishing y la verificación de URL antes de hacer clic en enlaces.

RustDuck (Botnet basada en Rust)

RustDuck es una nueva botnet desarrollada en el lenguaje Rust que secuestra routers, cámaras y servidores para lanzar ataques de Denegación de Servicio Distribuido (DDoS). Utiliza técnicas avanzadas para evadir la detección y expandir su red de dispositivos comprometidos.

MITRE ATT&CK: `T1498 — Network Denial of Service` `T1078 — Valid Accounts` `T1210 — Exploitation of Remote Services` `T1059.006 — Command and Scripting Interpreter: PowerShell`

> **Acción a seguir:** Asegure todos los dispositivos conectados a la red, incluyendo routers y cámaras IoT, con contraseñas fuertes y firmware actualizado. Monitoree el tráfico de red en busca de patrones de ataques DDoS y actividad inusual que pueda indicar una infección por botnet.

Ransomware de Navegador (Generado por IA)

Investigadores han descubierto un nuevo ransomware 'In-Browser' generado por IA (DeepSeek) que explota la API File System Access de Chromium en Windows, Linux, macOS y Android. Este ransomware puede robar y cifrar archivos directamente desde el navegador, afectando una amplia gama de sistemas operativos.

MITRE ATT&CK: `T1486 — Data Encrypted for Impact` `T1560.001 — Archive Collected Data: Archive via Utility` `T1574.008 — Hijack Execution Flow: DLL Side-Loading`

> **Acción a seguir:** Mantenga los navegadores Chromium y sus sistemas operativos actualizados. Configure los navegadores para restringir el acceso a APIs sensibles y eduque a los usuarios sobre los riesgos de descargar archivos o dar permisos a sitios web no confiables.

APT CL-STA-1062 (Backdoor TinyRCT)

El grupo APT de habla china CL-STA-1062 está utilizando la nueva puerta trasera (backdoor) 'TinyRCT' en ataques dirigidos a entidades gubernamentales e infraestructura crítica en Asia. Este malware permite el acceso persistente y el control remoto de sistemas comprometidos.

MITRE ATT&CK: `T1059.006 — Command and Scripting Interpreter: PowerShell` `T1547.001 — Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder` `T1090 — Proxy` `T1021.001 — Remote Services: Remote Desktop Protocol`

> **Acción a seguir:** Implemente soluciones de detección y respuesta de endpoints (EDR) y monitoreo de la red para identificar actividades sospechosas. Refuerce las políticas de acceso y segmentación de red para proteger los activos críticos y limitar la propagación lateral de posibles infecciones.

NOTICIAS DE CIBERSEGURIDAD

CVE-2026-55200 en libssh2: Vulnerabilidad Crítica en Clientes SSH con PoC Público

Se ha publicado una Prueba de Concepto (PoC) para CVE-2026-55200, una falla crítica en la biblioteca libssh2 que permite corrupción de memoria y ejecución de código arbitrario en clientes SSH. Esta vulnerabilidad afecta a múltiples aplicaciones que utilizan libssh2, poniendo en riesgo la confidencialidad e integridad de los sistemas.

Pedit COW: Nueva vulnerabilidad del kernel Linux permite acceso root a usuarios locales

Se ha descubierto la vulnerabilidad 'Pedit COW' (CVE-2026-46331) en el kernel de Linux. Esta falla permite a usuarios locales no privilegiados obtener acceso de root, lo que representa un riesgo significativo para la seguridad de los sistemas Linux. Es crucial aplicar las mitigaciones para evitar la escalada de privilegios.

Vulnerabilidad Crítica CVE-2026-46817 en Oracle E-Business Suite bajo Explotación Activa

Una falla crítica de seguridad (CVE-2026-46817) en Oracle E-Business Suite está siendo activamente explotada por actores maliciosos. Las empresas que utilizan este software deben parchear y monitorear sus sistemas de manera urgente para prevenir compromisos que podrían afectar operaciones críticas y datos sensibles.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice de inmediato el parcheo de SimpleHelp (CVE-2026-48558, crítica, plazo CISA 2026-07-02 ya vencido: actualice a 5.5.16 o superior, o deshabilite OIDC mientras tanto) y de Microsoft SharePoint Server (CVE-2026-45659, plazo 2026-07-04). Fortalezca el monitoreo de credenciales y acceso en dispositivos de red —especialmente FortiGate, ante la campaña FortiBleed y su vínculo con el ransomware INC— y audite permisos de aplicaciones de terceros en plataformas de colaboración. Refuerce además las defensas contra malware asistido por IA, phishing y botnets DDoS mediante soluciones EDR y concientización de usuarios. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) se encuentra alerta para detectar y mitigar cualquier actividad relacionada con las amenazas de esta edición.