INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W28 · 6 jul 2026 – 12 jul 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta edición semanal del Boletín de Ciberseguridad de Ingeniería Telemática S.A.S. destaca dos vulnerabilidades de alto impacto con explotación activa: una de path traversal en Adobe ColdFusion que puede derivar en ejecución de código, y una omisión de autorización en Langflow (plataforma de flujos de IA). El foco de la semana está en las amenazas: el framework de malware modular Avalon (con el ransomware CrownX), la técnica HalluSquatting que manipula asistentes de IA de codificación, el abuso de passkeys en Microsoft Entra para robar acceso a Microsoft 365, el backdoor destructivo GigaWiper y el ransomware GodDamn, que deshabilita soluciones EDR mediante un driver firmado (BYOVD).

1 Crítica 1 Alta

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

Publicado 13 jul 2026
Fuentes: CISA KEV, NVD y avisos de fabricante.

Ver detalle →

VISTA RÁPIDA

Severidad CVSS · explotación activa (CISA KEV)

1	1	0	0
Crítica	Alta	Media	Baja

2 vulnerabilidades con explotación activa confirmada · 5 campaña(s) de malware · 1 noticia(s)

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-48282

Adobe ColdFusion: Vulnerabilidad de Path Traversal

Adobe ColdFusion · CWE-22 · Versiones afectadas: ≤2023.20

Adobe ColdFusion presenta una vulnerabilidad de path traversal que podría permitir el acceso a rutas arbitrarias del sistema.

Impacto: La explotación de esta vulnerabilidad puede llevar a la ejecución arbitraria de código en el contexto del usuario actual, resultando en un compromiso significativo del sistema.

> **Acción a seguir:** Actualice Adobe ColdFusion a una versión superior a la 2023.20. El plazo de remediación de CISA es el 10 de julio de 2026.

Ampliar información: NVD — CVE-2026-48282 CISA KEV

Alta · CVSS 8.4 EXPLOTACIÓN ACTIVA CVE-2026-55255

Langflow: Omisión de Autorización por Clave Controlada por el Usuario

Langflow Langflow · CWE-288 · Versiones afectadas: < 1.9.1

Langflow contiene una vulnerabilidad de omisión de autorización que permite a un atacante autenticado ejecutar cualquier flujo perteneciente a otro usuario al especificar la ID de flujo de la víctima en la solicitud.

Impacto: Un atacante puede acceder y manipular flujos de trabajo de otros usuarios, comprometiendo la confidencialidad e integridad de la información y procesos de la aplicación.

> **Acción a seguir:** Actualice Langflow a la versión 1.9.1 o superior. El plazo de remediación de CISA es el 10 de julio de 2026.

Ampliar información: NVD — CVE-2026-55255 CISA KEV

MALWARE Y CAMPAÑAS

Avalon (Ransomware CrownX)

Avalon es un avanzado framework de malware modular que evade los controles de seguridad tradicionales. Utiliza técnicas de phishing para recolectar credenciales y desplegar el ransomware CrownX, afectando la disponibilidad y confidencialidad de los datos. La modularidad de Avalon le permite adaptarse y extender sus capacidades maliciosas.

MITRE ATT&CK: `T1566 — Phishing` `T1078 — Valid Accounts` `T1071 — Application Layer Protocol` `T1059 — Command and Scripting Interpreter` `T1486 — Data Encrypted for Impact`

> **Acción a seguir:** Implemente autenticación multifactor (MFA) en todos los servicios. Capacite a los usuarios para identificar y reportar intentos de phishing. Asegure los endpoints con soluciones EDR/XDR robustas capaces de detectar comportamientos evasivos y ransomware. Mantenga copias de seguridad de datos críticas de forma regular y aislada.

HalluSquatting

HalluSquatting es una nueva técnica de ataque que explota las 'alucinaciones' de los asistentes de inteligencia artificial (IA), como los de codificación, para engañarlos y que desplieguen malware, como botnets. Los atacantes manipulan los resultados de búsqueda o sugerencias de código que la IA podría generar de forma incorrecta, llevando a la instalación de software malicioso.

MITRE ATT&CK: `T1566 — Phishing` `T1204 — User Execution`

> **Acción a seguir:** Siempre valide el código y las sugerencias generadas por la IA con fuentes confiables y revise manualmente cualquier código antes de su ejecución. Implemente políticas de seguridad de desarrollo que incluyan revisiones de código y sandboxing para entornos de desarrollo.

Abuso de Passkeys en Microsoft Entra

Ciberdelincuentes están utilizando campañas de vishing y kits de phishing avanzados para engañar a usuarios de Microsoft 365. El objetivo es que los usuarios registren sus propias passkeys controladas por los atacantes en Microsoft Entra, obteniendo así acceso persistente y no autorizado a cuentas corporativas sin necesidad de contraseñas.

MITRE ATT&CK: `T1566 — Phishing` `T1078 — Valid Accounts` `T1550 — Use Alternate Authentication Material`

> **Acción a seguir:** Fortalezca la seguridad de identidad implementando MFA. Eduque a los usuarios sobre los riesgos de vishing y phishing, y la importancia de verificar siempre las solicitudes de autenticación. Monitoree activamente los registros de autenticación en Microsoft Entra para detectar registros de passkeys sospechosos o inusuales.

GigaWiper

GigaWiper es un backdoor destructivo para Windows, desarticulado por Microsoft, que combina capacidades de espionaje, borrado de datos (wiping) y la simulación de un ransomware. Este malware busca exfiltrar información sensible y, posteriormente, hacer que los sistemas sean inoperables, causando un daño significativo.

MITRE ATT&CK: `T1071 — Application Layer Protocol` `T1005 — Data from Local System` `T1083 — File and Directory Discovery` `T1486 — Data Encrypted for Impact` `T1490 — Inhibit System Recovery`

> **Acción a seguir:** Mantenga los sistemas operativos y todo el software actualizado con los últimos parches de seguridad. Implemente soluciones EDR/XDR robustas para la detección temprana de actividades maliciosas. Realice copias de seguridad de datos críticas de forma regular y asegúrese de que estén aisladas de la red de producción.

GodDamn Ransomware

El ransomware GodDamn se destaca por sus tácticas evasivas, utilizando el controlador malicioso 'PoisonX' (firmado por Microsoft) para deshabilitar soluciones EDR y antivirus. Esta técnica, conocida como BYOVD (Bring Your Own Vulnerable Driver), le permite operar sin ser detectado y cifrar datos corporativos.

MITRE ATT&CK: `T1562.001 — Impair Defenses: Disable or Modify Tools` `T1053 — Scheduled Task/Job` `T1486 — Data Encrypted for Impact`

> **Acción a seguir:** Implemente control de aplicaciones para restringir la ejecución de programas no autorizados y controladores desconocidos. Monitoree activamente la carga de controladores en sus sistemas. Utilice soluciones EDR/XDR con capacidades avanzadas de detección de BYOVD y protección contra la manipulación de agentes de seguridad.

NOTICIAS DE CIBERSEGURIDAD

Falla 'Rogue Agent' en Google Dialogflow CX permitía secuestro de chatbots y robo de datos

Se descubrió una falla crítica denominada 'Rogue Agent' en Google Dialogflow CX que permitía a atacantes con acceso privilegiado comprometer chatbots, robar datos sensibles y enviar mensajes falsos. Esta vulnerabilidad resaltó la importancia de asegurar las configuraciones de IA conversacional para prevenir el acceso no autorizado y la manipulación de información.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación de parches para Adobe ColdFusion y Langflow, ambas con explotación activa y plazo de CISA del 10 de julio de 2026. En el frente de amenazas, verifique que sus soluciones EDR/XDR estén afinadas para detectar TTPs de ransomware (CrownX, GodDamn, GigaWiper) y de abuso de identidad (phishing/vishing de Avalon y del abuso de passkeys en Microsoft Entra); active el control de aplicaciones y el monitoreo de carga de controladores para frenar técnicas BYOVD. Refuerce la validación del código sugerido por asistentes de IA para mitigar HalluSquatting. Nuestro SOC ofrece monitoreo y respuesta gestionada (FortiGuard SOCaaS) para ayudar a su organización a protegerse frente a estas y otras amenazas emergentes.