INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W33 · 10 ago 2026 – 16 ago 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta edición destaca la explotación activa de vulnerabilidades críticas y de alta severidad. Es crucial priorizar la aplicación de parches para una inyección SQL crítica en Metabase (CVSS 10.0) y una vulnerabilidad de denegación de servicio en Cisco Secure Firewall ASA y FTD (CVSS 8.6), ambas con un plazo de mitigación muy corto (14 de agosto de 2026). También se alerta sobre una vulnerabilidad de elevación de privilegios en Microsoft Windows AFD (CVSS 7.0) explotada activamente, incluyendo por el Grupo Lazarus. En el ámbito del malware, se observa la actividad del ransomware Gunra atacando infraestructura crítica, el desarrollo de capacidades de IA offline por el grupo Kimsuky, y la emergente botnet Kimwolf v7 especializada en ataques DDoS HTTP/2.

1 Crítica · 2 Alta

Publicado 17 ago 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	2	0	0
Crítica	Alta	Media	Baja

3 vulnerabilidades con explotación activa confirmada · 3 campaña(s) de malware · 5 noticia(s)

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-72898

Inyección SQL Crítica en Metabase

Metabase Metabase · CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') · Versiones afectadas: `x.58.0 - <x.58.24; x.59.0 - <x.59.21; x.60.0 - <x.60.17; x.61.0 - <x.61.11`

Esta vulnerabilidad de inyección SQL permite a un atacante remoto no autenticado inyectar SQL arbitrario en la base de datos de la aplicación Metabase. La explotación exitosa puede otorgar acceso de administrador a la instancia.

Impacto: Un atacante podría obtener control total sobre la instancia de Metabase, modificar la configuración de la aplicación, robar datos almacenados y comprometer la integridad y confidencialidad de la información.

> **Acción a seguir:** Actualice Metabase a la versión 0.58.24, 0.59.21, 0.60.17, 0.61.11 o posterior. La fecha límite de CISA para aplicar la mitigación es el 14 de agosto de 2026.

Ampliar información: NVD — CVE-2026-72898 CISA KEV

Alta · CVSS 8.6 EXPLOTACIÓN ACTIVA CVE-2026-20349

Vulnerabilidad de Denegación de Servicio en Cisco Secure Firewall ASA y FTD

Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) · CWE-400: Uncontrolled Resource Consumption · Versiones afectadas: `9.16.1; 9.16.1.28; 9.16.2; 9.16.2.3; 9.16.2.7`

Una vulnerabilidad de inspección de heap en Cisco Secure Firewall Adaptive Security Appliance (ASA) y Secure Firewall Threat Defense (FTD) podría permitir a un atacante remoto no autenticado provocar una recarga inesperada del dispositivo.

Impacto: La explotación resulta en una condición de denegación de servicio (DoS), afectando la disponibilidad de los servicios protegidos por los firewalls Cisco.

> **Acción a seguir:** Actualice los dispositivos afectados a las versiones parcheadas para mitigar la vulnerabilidad. La fecha límite de CISA para aplicar la mitigación es el 14 de agosto de 2026. Consulte la documentación oficial de Cisco para las versiones específicas que corrigen este fallo.

Ampliar información: NVD — CVE-2026-20349 CISA KEV

Alta · CVSS 7.0 EXPLOTACIÓN ACTIVA CVE-2026-68820

Vulnerabilidad de Uso Después de Liberación en Microsoft Windows Ancillary Function Driver para WinSock

Microsoft Windows Ancillary Function Driver for WinSock · CWE-416: Use-After-Free · Versiones afectadas: `10.0.14393.0 – <10.0.14393.9418; 10.0.17763.0 – <10.0.17763.9115; 10.0.19044.0 – <10.0.19044.7663; 10.0.19045.0 – <10…`

Microsoft Windows Ancillary Function Driver para WinSock contiene una vulnerabilidad de uso después de liberación que permite a un atacante local autenticado elevar privilegios en el sistema. Se ha observado su explotación activa por parte del Grupo Lazarus a través de técnicas de ingeniería social para obtener acceso SYSTEM y desplegar backdoors.

Impacto: Un atacante con acceso inicial al sistema podría escalar sus privilegios a SYSTEM, obteniendo control total sobre el dispositivo y facilitando la persistencia y el despliegue de malware.

> **Acción a seguir:** Aplique los parches de seguridad de Microsoft publicados en el ciclo de actualizaciones. La fecha límite de CISA para aplicar la mitigación es el 25 de agosto de 2026. Asegúrese de que los sistemas Windows estén actualizados con las últimas correcciones de seguridad.

Ampliar información: NVD — CVE-2026-68820 CISA KEV

MALWARE Y CAMPAÑAS

Gunra Ransomware

CISA y el FBI han alertado sobre el ransomware Gunra, que explota vulnerabilidades en productos Fortinet y Schneider Electric para atacar infraestructura crítica. Este grupo utiliza tácticas de doble extorsión, cifrando datos y amenazando con su publicación, y emplea técnicas avanzadas para evadir la detección y maximizar el impacto.

MITRE ATT&CK: `T1486 — Data Encrypted for Impact` `T1071.001 — Application Layer Protocol: Web Protocols` `T1190 — Exploit Public-Facing Application`

> **Acción a seguir:** Implemente segmentación de red, MFA robusta y parches de seguridad para Fortinet y Schneider Electric. Realice copias de seguridad regularmente y manténgalas aisladas. Capacite al personal en detección de phishing. Fortalezca la vigilancia de los sistemas expuestos a internet, especialmente aquellos de infraestructura crítica.

Kimsuky (Ataques con IA offline)

El grupo norcoreano Kimsuky está desarrollando y utilizando una pila de inteligencia artificial (IA) offline para crear campañas de phishing altamente sofisticadas e indetectables y automatizar el desarrollo de malware. Esta capacidad les permite generar contenido malicioso de forma autónoma, sin depender de servicios en la nube o conexiones a internet, lo que dificulta su rastreo y bloqueo.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1588 — Obtain Capabilities` `T1071.001 — Application Layer Protocol: Web Protocols`

> **Acción a seguir:** Mejore las defensas de correo electrónico con filtros avanzados y análisis de comportamiento. Implemente soluciones de detección de amenazas basadas en IA y machine learning. Eduque a los usuarios sobre los riesgos del phishing avanzado. Considere la seguridad de la cadena de suministro de software y hardware para detectar posibles compromisos.

Kimwolf v7 Botnet

Se ha descubierto la botnet Kimwolf v7, una nueva amenaza que infecta dispositivos Android e IoT. Esta botnet es capaz de lanzar ataques de denegación de servicio distribuido (DDoS) HTTP/2 y camuflar su tráfico malicioso como actividad legítima, dificultando su detección por parte de las defensas de red.

MITRE ATT&CK: `T1499 — Endpoint Denial of Service` `T1105 — Ingress Tool Transfer` `T1071.001 — Application Layer Protocol: Web Protocols`

> **Acción a seguir:** Asegure todos los dispositivos IoT y Android con las últimas actualizaciones de seguridad. Implemente segmentación de red para limitar el impacto de un posible compromiso. Utilice soluciones DDoS que puedan analizar el tráfico HTTP/2 y diferenciar entre el tráfico legítimo y los ataques camuflados. Monitoree patrones de tráfico anómalos en sus redes.

NOTICIAS DE CIBERSEGURIDAD

Explotación activa de vulnerabilidad crítica en VMware vCenter: CVE-2026-59310

Una vulnerabilidad crítica (CVE-2026-59310) en VMware vCenter está siendo explotada activamente, permitiendo a los atacantes obtener acceso remoto persistente. Se insta a las organizaciones a aplicar los parches de seguridad de inmediato para mitigar el riesgo.

ShieldBreak: Bypass de Zero-Day en Microsoft Defender con Acceso SYSTEM Revelado

Un investigador de seguridad ha revelado 'ShieldBreak', un bypass de zero-day que elude el parche previamente emitido por Microsoft Defender para la vulnerabilidad RoguePlanet (CVE-2026-50656). Este bypass permite a los atacantes obtener acceso SYSTEM, lo que representa una grave amenaza a la seguridad de los sistemas Windows.

Cisco parcha vulnerabilidades críticas en SD-WAN, IOS XE e IMC

Cisco ha lanzado actualizaciones de seguridad para corregir doce vulnerabilidades críticas que afectan a sus plataformas Catalyst SD-WAN, IOS XE e Integrated Management Controller (IMC). Tres de estas vulnerabilidades tienen puntuaciones CVSS de hasta 9.9, destacando la urgencia de aplicar los parches para proteger la infraestructura de red.

Nuevos ataques a Passkeys: Amenazas a la autenticación sin contraseñas y MFA

Investigadores de seguridad han revelado métodos para bypassar Passkeys y la autenticación multifactor (MFA) en entornos de Windows, Entra ID y Chrome. Estos hallazgos ponen de manifiesto desafíos emergentes para la autenticación sin contraseñas y subrayan la importancia de una gestión robusta de identidad y un MFA contextual para proteger los activos empresariales.

Cadena de exploits en SharePoint permite ejecución remota de código sin autenticación (RCE)

Se ha descubierto y están siendo explotadas activamente una cadena de vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2026-55040 y CVE-2026-63520). Estas vulnerabilidades permiten la ejecución remota de código (RCE) sin necesidad de autenticación, especialmente tras la publicación de pruebas de concepto (PoC) públicas. Es imperativo aplicar los parches disponibles de inmediato.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice urgentemente la aplicación de parches para Metabase (CVE-2026-72898) y Cisco Secure Firewall ASA/FTD (CVE-2026-20349) antes del 14 de agosto de 2026. A continuación, proceda con las actualizaciones para Microsoft Windows AFD (CVE-2026-68820) antes del 25 de agosto de 2026. Mantenga sus soluciones de seguridad perimetral Fortinet actualizadas y preste especial atención a las alertas sobre Gunra Ransomware, Kimsuky y la botnet Kimwolf v7. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a las TTPs asociadas a estas amenazas para proteger su infraestructura.

AVISO: Boletín informativo TLP:CLEAR de Ingeniería Telemática S.A.S. Datos provenientes de CISA KEV, NVD y avisos de fabricante. De carácter informativo; no sustituye un análisis de su entorno.