INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W34 · SEMANAL

Semana del 17 ago 2026 al 23 ago 2026 · publicado el 24 de agosto de 2026

Boletín de Ciberseguridad

Las vulnerabilidades con explotación activa, las campañas de malware y las noticias de la semana, en español y con acciones concretas para su empresa.

RESUMEN EJECUTIVO

Esta semana, el Boletín de Ciberseguridad destaca una alta criticidad debido a múltiples vulnerabilidades activamente explotadas en productos clave de infraestructura como Broadcom VMware vCenter, Microsoft IKE, Apple macOS y Microsoft SharePoint, todas con plazos de parcheo inmediatos por parte de CISA. En particular, la vulnerabilidad en VMware vCenter ya está siendo utilizada por actores APT para desplegar ransomware Babuk. Además, se observa una intensa actividad de malware, incluyendo el avanzado rootkit CoolClient de Mustang Panda, el implante TWINLOOT que abusa de Microsoft 365, nuevas variantes de malware bancario para Android como ToxicPanda 2.0 y GoldDigger, y ataques a la cadena de suministro de Rust. La situación exige una respuesta rápida en la aplicación de parches y un monitoreo robusto de las amenazas persistentes.

8	8	7
VULNERABILIDADES	CON EXPLOTACIÓN ACTIVA	CAMPAÑAS DE MALWARE

Ciberseguridad 360°
Protección avanzada con Fortinet.

Nube híbrida
AWS, Azure, Google Workspace, M365.

Continuidad (DRP)
Veeam y Acronis.

SOC gestionado
Monitoreo y respuesta.

Boletín informativo de distribución pública (TLP:CLEAR).
Fuentes: CISA KEV, NVD y avisos de fabricante. No sustituye un análisis de su entorno.

Ver detalle →

NIT 816007833-0 · Pereira, Colombia · +57 314 682 5259 · ingenieriatelematica.com.co · soporte@ingetele.com

VISTA RÁPIDA

severidad CVSS · explotación activa según CISA KEV

8	0	0	0
CRÍTICA	ALTA	MEDIA	BAJA
CVSS 9,0 – 10	CVSS 7,0 – 8,9	CVSS 4,0 – 6,9	CVSS 0,1 – 3,9

8 vulnerabilidades, 8 con explotación activa confirmada · 7 campaña(s) de malware · 6 noticia(s) · semana del 17 ago 2026 al 23 ago 2026

VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-59310

Broadcom VMware vCenter Vulnerabilidad de Recorrido de Ruta

Broadcom VMware vCenter · CWE-22 — Path Traversal · Versiones afectadas: `9.1.x.x; 9.0.x.x; 5.x; 9.1.x.x - <9.1.0.0300; 9.0.x.x - <9.0.2.0100`

Una vulnerabilidad de recorrido de ruta en Broadcom VMware vCenter permite a un atacante con acceso a la red ejecutar código arbitrario. Esta vulnerabilidad está siendo activamente explotada por actores vinculados a China para desplegar ransomware Babuk, afectando a cientos de organizaciones.

Impacto: Ejecución remota de código arbitrario (RCE), que puede llevar al compromiso total del sistema y al despliegue de ransomware.

> **Acción a seguir:** Actualizar las versiones afectadas de VMware vCenter a las versiones parcheadas (9.1.0.0300, 9.0.2.0100 o superiores) antes del 21 de agosto de 2026.

Ampliar información: NVD — CVE-2026-59310 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-33824

Microsoft IKE Service Extensions Vulnerabilidad Double Free

Microsoft Internet Key Exchange (IKE) Service Extensions · CWE-416 — Use-After-Free · Versiones afectadas: `10.0.14393.0 - <10.0.14393.9060; 10.0.17763.0 - <10.0.17763.8644; 10.0.19044.0 - <10.0.19044.7184; 10.0.19045.0 - <10…`

Las extensiones del servicio Microsoft Internet Key Exchange (IKE) contienen una vulnerabilidad de doble liberación de memoria (double free) que podría permitir la ejecución remota de código.

Impacto: Ejecución remota de código arbitrario (RCE) en el sistema afectado, llevando al compromiso completo del servicio IKE.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft para las versiones afectadas (anteriores a 10.0.14393.9060, 10.0.17763.8644, 10.0.19044.7184, etc.) antes del 21 de agosto de 2026.

Ampliar información: NVD — CVE-2026-33824 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-65400

Apple macOS Vulnerabilidad de Autenticación Impropia

Apple macOS · CWE-287 — Improper Authentication · Versiones afectadas: `<14.8.9; <15.7.9; <26.6.1`

Una vulnerabilidad de autenticación impropia en Apple macOS permite a un atacante en la red autenticarse en Screen Sharing sin credenciales válidas.

Impacto: Acceso no autorizado a Screen Sharing, que podría llevar al control remoto del sistema afectado.

> **Acción a seguir:** Actualizar macOS a las versiones 14.8.9, 15.7.9, 26.6.1 o superiores antes del 21 de agosto de 2026.

Ampliar información: NVD — CVE-2026-65400 CISA KEV

Crítica · CVSS 9.5 Explotación activa CVE-2026-72530

TrueConf Server Vulnerabilidad de Inyección de Código

TrueConf Server · CWE-94 — Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `* - <5.3; 5.3 - <5.3.9; 5.4 - <5.4.9; 5.5 - <5.5.5`

Una vulnerabilidad de inyección de código en TrueConf Server podría permitir a un atacante remoto no autorizado con acceso a la red (puerto 4307/TCP) ejecutar scripts maliciosos para escapar del entorno aislado y ejecutar código arbitrario en el sistema host.

Impacto: Ejecución remota de código arbitrario (RCE) en el servidor, lo que puede llevar al compromiso total del sistema.

> **Acción a seguir:** Actualizar TrueConf Server a las versiones 5.3.9, 5.4.9, 5.5.5 o superiores antes del 03 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-72530 CISA KEV

Crítica · CVSS 9.4 Explotación activa CVE-2025-62593

Ray-Project Ray Vulnerabilidad de Inyección de Código

Ray-Project Ray · CWE-94 — Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `< 2.52.0`

Ray-Project Ray contiene una vulnerabilidad de inyección de código que podría permitir la ejecución remota de código. Desarrolladores que usan Ray como herramienta de desarrollo pueden estar expuestos, siendo explotable a través de Firefox y Safari.

Impacto: Ejecución remota de código arbitrario (RCE), permitiendo a un atacante tomar control del sistema que ejecuta Ray.

> **Acción a seguir:** Actualizar Ray-Project Ray a la versión 2.52.0 o superior antes del 20 de agosto de 2026.

Ampliar información: NVD — CVE-2025-62593 CISA KEV

Crítica · CVSS 9.3 Explotación activa CVE-2026-72529

TrueConf Server Vulnerabilidad por Falta de Autenticación para Función Crítica

TrueConf Server · CWE-306 — Missing Authentication for Critical Function · Versiones afectadas: `* - <5.3; 5.3 - <5.3.9; 5.4 - <5.4.9; 5.5 - <5.5.5`

TrueConf Server presenta una vulnerabilidad por falta de autenticación para una función crítica, permitiendo a un atacante remoto no autorizado con acceso a la red (puerto 4307/TCP) ejecutar un script arbitrario.

Impacto: Ejecución de scripts arbitrarios sin autenticación, que podría llevar a la toma de control del sistema o exfiltración de datos.

> **Acción a seguir:** Actualizar TrueConf Server a las versiones 5.3.9, 5.4.9, 5.5.5 o superiores antes del 23 de agosto de 2026.

Ampliar información: NVD — CVE-2026-72529 CISA KEV

Crítica · CVSS 9.3 Explotación activa CVE-2026-64849

MLflow Server-Side Request Forgery (SSRF)

MLflow MLflow · CWE-918 — Server-Side Request Forgery (SSRF) · Versiones afectadas: `< 3.15.0`

MLflow contiene una vulnerabilidad de Server-Side Request Forgery (SSRF) que puede permitir a los atacantes alcanzar servicios internos o metadatos en la nube y recibir el estado y cuerpo de la respuesta.

Impacto: Acceso no autorizado a información sensible de sistemas internos o servicios en la nube, con potencial para escalada de privilegios.

> **Acción a seguir:** Actualizar MLflow a la versión 3.15.0 o superior antes del 02 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-64849 CISA KEV

Crítica · CVSS 9.1 Explotación activa CVE-2026-55040

Microsoft SharePoint Vulnerabilidad de Autenticación Débil

Microsoft SharePoint · CWE-287 — Improper Authentication · 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 autenticación débil que permite a un atacante no autorizado eludir una función de seguridad a través de la red.

Impacto: Elusión de mecanismos de seguridad, llevando a acceso no autorizado a datos o funcionalidades de SharePoint.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft para las versiones afectadas (anteriores a 16.0.5561.1001, 16.0.10417.20175, 16.0.19725.20434, etc.) antes del 21 de agosto de 2026.

Ampliar información: NVD — CVE-2026-55040 CISA KEV

MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

CoolClient (familia Mustang Panda/HoneyMyte)

El grupo de APT Mustang Panda (también conocido como HoneyMyte) ha actualizado su malware CoolClient con un rootkit en modo kernel de Windows. Este rootkit, firmado digitalmente, permite una evasión avanzada de detección, dificultando su identificación por soluciones de seguridad estándar.

MITRE ATT&CK `T1548.001 — Bypass User Account Control: Signed Binary Proxy Execution` `T1070.006 — Indicator Removal: Timestomp` `T1562 — Impair Defenses`

> **Acción a seguir:** Implementar soluciones EDR/XDR robustas con capacidades de detección a nivel de kernel y monitoreo continuo. Realizar auditorías de integridad de archivos y certificados de controladores.

Ampliar información: Mustang Panda Potencia CoolClient con Rootkit Firmado en Windows para Evasión Avanzada

TWINLOOT

Se ha descubierto TWINLOOT, un nuevo implante escrito en Python diseñado para explotar Microsoft 365. Este malware utiliza SharePoint y Teams para establecer canales de comando y control (C2) y robar credenciales.

MITRE ATT&CK `T1071.001 — Application Layer Protocol: Web Protocols` `T1566 — Phishing` `T1003 — OS Credential Dumping`

> **Acción a seguir:** Fortalecer la seguridad de Microsoft 365 con MFA, monitoreo de actividad sospechosa en SharePoint y Teams, y utilizar soluciones EDR/XDR para detectar comportamiento anómalo.

Ampliar información: TWINLOOT: Nuevo Malware Python que Explota Microsoft 365 para Robo de Credenciales

ToxicPanda 2.0 y GoldDigger

ToxicPanda 2.0 y GoldDigger son variantes de malware bancario para Android que están expandiendo sus ataques. Emplean técnicas de fraude en dispositivo, superposiciones (overlays) para engañar a los usuarios y abuso de la función de accesibilidad de Android para tomar el control de los dispositivos y realizar transacciones fraudulentas.

MITRE ATT&CK `T1401 — Obtain Device Information` `T1056.001 — Input Capture: Keylogging` `T1056.002 — Input Capture: GUI Input Capture`

> **Acción a seguir:** Educar a los usuarios sobre los riesgos del sideloading de aplicaciones. Implementar soluciones de seguridad móvil (MDR/XDR para móviles) y mantener los sistemas operativos de los dispositivos actualizados.

Ampliar información: ToxicPanda 2.0 y GoldDigger: Nuevas Amenazas de Malware Bancario Android con Fraude en Dispositivos

PATCHCORD y SHEETCORD (APT36)

Una nueva campaña atribuida al grupo de amenazas persistentes avanzadas (APT36) está desplegando las backdoors PATCHCORD y SHEETCORD. Estas herramientas maliciosas están dirigidas a organizaciones de telecomunicaciones afganas e infraestructura crítica en la India.

MITRE ATT&CK `T1071.001 — Application Layer Protocol: Web Protocols` `T1070.004 — Indicator Removal on Host: File Deletion` `T1059 — Command and Scripting Interpreter` `T1021 — Remote Services`

> **Acción a seguir:** Fortalecer las defensas perimetrales y de red. Implementar segmentación de red y monitoreo exhaustivo para detectar tráfico anómalo o comunicaciones C2 con estas backdoors.

Ampliar información: Nuevas Backdoors PATCHCORD y SHEETCORD atacan Telcos y Crítica Infraestructura en Asia

UNC6293, UNC7005 y UNC5976 (Hackers Rusos)

Grupos de ciberespionaje vinculados a Rusia, identificados como UNC6293, UNC7005 y UNC5976, están explotando la funcionalidad de Google OAuth y la vinculación de cuentas de WhatsApp para secuestrar cuentas de usuarios. Estos ataques se enfocan en la protección de la identidad y la eficacia de la autenticación multifactor (MFA).

MITRE ATT&CK `T1566.002 — Phishing: Spearphishing Link` `T1078.004 — Valid Accounts: Cloud Accounts` `T1114.001 — Email Collection: Local Email Collection`

> **Acción a seguir:** Revisar la configuración de permisos de aplicaciones de terceros en Google OAuth. Reforzar la formación de concienciación sobre phishing y el uso de MFA en todas las cuentas corporativas.

Ampliar información: Hackers Rusos Abusan Google OAuth y WhatsApp: Impacto en Seguridad de Cuentas Corporativas

WindRelay

WindRelay es un nuevo malware para Android que, en combinación con SpyNote, transforma los dispositivos infectados en relés NFC para ejecutar fraudes de pagos sin contacto y robar datos de tarjetas. Esto permite a los atacantes realizar transacciones fraudulentas directamente desde los dispositivos comprometidos.

MITRE ATT&CK `T1040 — Network Sniffing` `T1003 — OS Credential Dumping` `T1552.001 — Unsecured Credentials: Credentials in Files`

> **Acción a seguir:** Educar a los usuarios sobre las amenazas móviles. Implementar soluciones de seguridad para dispositivos móviles (MDM/MDR) que detecten aplicaciones maliciosas y comportamientos sospechosos.

Ampliar información: WindRelay: Nuevo Malware Android Usa Teléfonos como Relés NFC para Fraude de Pagos

Ataque a la cadena de suministro de Rust

Un ataque a la cadena de suministro en el ecosistema de Rust ha inyectado malware en 'crates' (paquetes) populares como 'arrayref', afectando a compilaciones con millones de descargas. Esto compromete la integridad del código fuente y puede llevar a la ejecución de código malicioso en entornos de desarrollo y producción.

MITRE ATT&CK `T1195.002 — Supply Chain Compromise: Compromise Software Dependencies and Development Tools` `T1547.001 — Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder`

> **Acción a seguir:** Validar la integridad de todas las dependencias de software. Utilizar escaneo de seguridad en la cadena de suministro de software (SCA) y monitoreo de la integridad de los 'crates' utilizados.

Ampliar información: Ataque a la cadena de suministro de Rust compromete paquetes con millones de descargas

NOTICIAS DE CIBERSEGURIDAD

lo que cambia esta semana

Nueva cadena de exploits Unisoc VoLTE permite acceso total al kernel de Android sin parche

Investigadores han descubierto una cadena de exploits de dos etapas que otorga acceso total al kernel de Android en dispositivos equipados con chipsets Unisoc, explotable a través de llamadas VoLTE. Actualmente, no existe un parche disponible para esta vulnerabilidad, lo que representa un riesgo significativo para millones de dispositivos.

Ampliar información: Nueva cadena de exploits Unisoc VoLTE permite acceso total al kernel de Android sin parche

Vulnerabilidad Crítica de RCE en Microsoft Entra ID (CVSS 10.0)

Se ha reportado una vulnerabilidad crítica (CVE-2026-69836) de ejecución remota de código en Microsoft Entra ID con un CVSS de 10.0. Aunque Microsoft ya ha mitigado esta vulnerabilidad, su existencia subraya la importancia de la gestión de identidades y la monitorización continua de la seguridad en entornos de nube.

Ampliar información: Vulnerabilidad Crítica de RCE en Microsoft Entra ID (CVSS 10.0) Explotada en Ataques Reales

Scripts de IA Explotan PLCs Siemens S7 en Infraestructura Crítica

El gobierno de EE. UU. ha emitido una alerta sobre la detección de scripts basados en inteligencia artificial que están siendo utilizados para atacar PLCs Siemens S7 en entornos de infraestructura crítica. Esta nueva técnica eleva el riesgo para los sistemas de tecnología operativa (OT) y destaca la necesidad de defensas específicas para estos entornos.

Ampliar información: Scripts de IA Explotan PLCs Siemens S7 en Infraestructura Crítica

Vulnerabilidad Zero-Day Crítica en GeoServer: Inyección SQL y RCE

Se ha identificado y se encuentra en explotación activa una vulnerabilidad zero-day crítica (GHSA-mqjf-5f49-2fjh) en GeoServer. Esta falla permite inyección SQL y ejecución remota de código (RCE), comprometiendo seriamente la integridad y disponibilidad de los datos y sistemas que utilizan GeoServer.

Ampliar información: Vulnerabilidad Zero-Day Crítica en GeoServer: Inyección SQL y RCE en Explotación Activa

Explotación activa de CVE-2026-58231 en SAP Commerce Cloud tras su parche

Días después de la publicación de un parche, se han detectado intentos de explotación activa de la vulnerabilidad crítica CVE-2026-58231 (CVSS 10.0) en SAP Commerce Cloud. Esta situación subraya la urgencia de aplicar parches inmediatamente al ser liberados, ya que los atacantes monitorean de cerca los avisos de seguridad.

Ampliar información: Explotación activa de CVE-2026-58231 en SAP Commerce Cloud tras su parche

Fuga de JWT en Cloudflare Workers: Ataque Spectre explota aislamiento en la nube

Investigadores han revelado un ataque Spectre que logró filtrar JSON Web Tokens (JWTs) de Cloudflare Workers a una tasa de 12 bits por segundo. Este incidente destaca la persistencia de las vulnerabilidades de canal lateral en entornos de computación en la nube y la complejidad de mantener el aislamiento de procesos seguro. La vulnerabilidad ya ha sido mitigada por Cloudflare.

Ampliar información: Fuga de JWT en Cloudflare Workers: Ataque Spectre explota aislamiento en la nube

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Dada la criticidad y explotación activa de múltiples vulnerabilidades, la acción prioritaria es aplicar los parches para Broadcom VMware vCenter (CVE-2026-59310), Microsoft IKE (CVE-2026-33824), Apple macOS (CVE-2026-65400) y Microsoft SharePoint (CVE-2026-55040) antes del 21 de agosto de 2026. Seguidamente, actualizar Ray-Project Ray (CVE-2025-62593) antes del 20 de agosto y TrueConf Server (CVE-2026-72529) antes del 23 de agosto. Para las vulnerabilidades con plazos más extensos (MLflow y TrueConf Server), se recomienda no demorar su aplicación. En cuanto a las amenazas de malware, es crucial implementar EDR/XDR para detectar rootkits como CoolClient y el comportamiento de TWINLOOT en Microsoft 365, así como monitorear la infraestructura crítica y dispositivos móviles ante amenazas como PATCHCORD/SHEETCORD, ToxicPanda/GoldDigger y WindRelay. Fortalecer la autenticación multifactor y la concienciación sobre phishing es esencial para contrarrestar campañas como las de los hackers rusos. Nuestro equipo de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a la actividad relacionada con estas amenazas para proteger sus activos.

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.