INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W42 · SEMANAL

Semana del 12 oct 2026 al 18 oct 2026 · publicado el 19 de octubre 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 edición del Boletín Semanal destaca múltiples vulnerabilidades críticas y de alta severidad, varias de ellas bajo explotación activa, afectando a productos clave como Cisco Secure Email Gateway, Atlassian, Microsoft Windows, Palo Alto Networks PAN-OS e Ivanti Connect Secure. Es crucial abordar estas vulnerabilidades con urgencia, especialmente aquellas con plazos inminentes para el parcheo. También se alerta sobre nuevas campañas de malware como 'Midnight Mimosa' y 'Hirudo' que impactan dispositivos Android, y la desarticulación de kits de phishing que han facilitado miles de millones de mensajes fraudulentos. Mantener los sistemas actualizados y robustecer las defensas de punto final y de red es prioritario.


| 16 | 12 | 3 |
|---|---|---|
| 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

| 12 | 3 | 1 | 0 |
|---|---|---|---|
| CRÍTICA | ALTA | MEDIA | BAJA |
| CVSS 9,0 – 10 | CVSS 7,0 – 8,9 | CVSS 4,0 – 6,9 | CVSS 0,1 – 3,9 |

16 vulnerabilidades, 12 con explotación activa confirmada · 3 campaña(s) de malware · 1 noticia(s) · semana del 12 oct 2026 al 18 oct 2026

## VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 10.0 **Explotación activa** CVE-2026-105134

### Falla de Inyección de Comandos en Ahsay AhsayCBS

Ahsay AhsayCBS · CWE-77: Command Injection · Versiones afectadas: `10.3.0; 10.3.1; 10.3.2`

Ahsay AhsayCBS contiene una vulnerabilidad de inyección de comandos que podría permitir a un atacante remoto ejecutar comandos del sistema operativo. Esto se logra manipulando el parámetro 'random' en el componente Replication Receiver, específicamente en el endpoint /rps/api/json/UpdateReceivers.do.

**Impacto:** Un atacante no autenticado puede lograr la ejecución remota de código con privilegios elevados, comprometiendo completamente el sistema afectado.

> **Acción a seguir:** Actualice a las versiones parcheadas tan pronto como estén disponibles. CISA ha establecido un plazo para la remediación antes del 17 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-105134 CISA KEV

Crítica · CVSS 10.0 **Explotación activa** Sin CVE asignado

### Explotación Activa de RCE (CVSS 10.0) en Bricksforge de WordPress

Bricksforge (Plugin de WordPress) · CWE-94: Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `Todas las versiones afectadas (se recomienda consultar al proveedor)`

Una vulnerabilidad crítica con CVSS 10.0 ha sido descubierta y está siendo activamente explotada en el plugin Bricksforge de WordPress. Esta falla permite la ejecución remota de código (RCE) no autenticada.

**Impacto:** La explotación exitosa permite a un atacante obtener control total sobre el sitio web, comprometer datos y realizar acciones maliciosas sin necesidad de credenciales.

> **Acción a seguir:** Parchee el plugin Bricksforge de WordPress urgentemente a la última versión disponible. Implemente y mantenga un Web Application Firewall (WAF) para mitigar intentos de explotación.

**Ampliar información:** Alerta Crítica: Explotación Activa de Vulnerabilidad RCE (CVSS 10.0) en Bricksforge de WordPress

Crítica · CVSS 10.0 Sin CVE asignado

### Vulnerabilidad Crítica (CVSS 10.0) en SAP Cloud SDK para Python Permite Robo de Credenciales OAuth2

SAP Cloud SDK para Python · CWE-287: Improper Authentication · Versiones afectadas: `Se recomienda consultar la documentación oficial de SAP para versiones afectadas.`

Se ha revelado una vulnerabilidad crítica con CVSS 10.0 en el Cloud SDK de SAP para Python. Esta falla permite el robo de credenciales OAuth2, afectando la seguridad de las aplicaciones que utilizan el SDK.

**Impacto:** Un atacante podría obtener credenciales OAuth2, permitiéndole el acceso no autorizado a recursos y datos protegidos en entornos SAP Business Technology Platform (BTP).

> **Acción a seguir:** Actualice el SAP Cloud SDK para Python a la versión más reciente. Revise y fortalezca los mecanismos de autenticación y autorización en sus aplicaciones SAP BTP.

**Ampliar información:** Vulnerabilidad crítica en SAP Cloud SDK para Python permite robo de credenciales OAuth2

Crítica · CVSS 9.8 Explotación activa CVE-2026-76519

## Vulnerabilidad de Recorrido de Ruta Relativa en Cisco Secure Email Gateway

Cisco Secure Email Gateway · CWE-23: Relative Path Traversal · Versiones afectadas: `14.0.0-698; 13.5.1-277; 13.0.0-392; 14.2.0-620; 13.0.5-007`

Cisco Secure Email Gateway contiene una vulnerabilidad de recorrido de ruta relativa que podría permitir a un atacante remoto no autenticado escribir archivos arbitrarios en el sistema operativo subyacente. Esta vulnerabilidad está siendo activamente explotada.

**Impacto:** Un atacante puede ejecutar código con privilegios de root, lo que lleva a un compromiso completo del dispositivo y la red.

> **Acción a seguir:** Aplique los parches de seguridad de Cisco a las versiones mencionadas. El plazo de CISA para la remediación es el 17 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-76519 CISA KEV

Crítica · CVSS 9.3 Explotación activa CVE-2026-21589

## Vulnerabilidad de Archivos o Directorios Accesibles a Partes Externas en Atlassian Multiple Products

Atlassian Multiple Products (Bitbucket, Confluence, Jira, Bamboo, Crowd, Crucible, Fisheye Data Center) · CWE-530: Exposure of Private Information Through Timing Discrepancy · Versiones afectadas: `Todas las demás versiones`

Múltiples productos de Atlassian Data Center y Server (Bitbucket, Confluence, Jira Service Management, Jira Software, Bamboo, Crowd, Crucible y Fisheye) contienen una vulnerabilidad que expone archivos o directorios a partes externas.

**Impacto:** Un atacante no autenticado podría acceder a información sensible o configuraciones internas de los productos, lo que podría llevar a un compromiso posterior o a la divulgación de datos.

> **Acción a seguir:** Aplique los parches de seguridad proporcionados por Atlassian para mitigar esta vulnerabilidad. El plazo de CISA para la remediación es el 18 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-21589 CISA KEV

Crítica · CVSS 9.3 Explotación activa CVE-2026-102764

## Vulnerabilidad de Bypass de Autenticación por Spoofing en BeyondTrust Remote Support

BeyondTrust Remote Support · CWE-288: Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: `≤26.2.3`

BeyondTrust Remote Support contiene una vulnerabilidad de bypass de autenticación por spoofing que podría permitir a un atacante remoto realizar operaciones de archivos en el appliance sin autenticación.

**Impacto:** Un atacante no autenticado puede manipular o eliminar archivos en el sistema, lo que podría llevar a la denegación de servicio o a la ejecución de código arbitrario.

> **Acción a seguir:** Actualice BeyondTrust Remote Support a una versión posterior a la 26.2.3. CISA ha establecido un plazo para la remediación antes del 19 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-102764 CISA KEV

Crítica · CVSS n/d CVE-2026-108097

## Vulnerabilidad Crítica de Ejecución Remota de Código (RCE) sin Autenticación en Drupal Field UI

Drupal (módulo Field UI) · CWE-94: Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `Actualice a las versiones 11.4.10, 11.3.19 o 10.6.19`

Una falla crítica en el módulo Field UI de Drupal posibilita la ejecución remota de código (RCE) sin autenticación, lo que representa un riesgo significativo para la seguridad de los sitios web afectados.

**Impacto:** Un atacante puede ejecutar código arbitrario en el servidor, obteniendo control total sobre el sitio Drupal y los datos asociados.

> **Acción a seguir:** Actualice urgentemente sus instalaciones de Drupal a las versiones 11.4.10, 11.3.19 o 10.6.19 para mitigar esta vulnerabilidad.

**Ampliar información:** NVD — CVE-2026-108097 CISA KEV

Crítica · CVSS n/d Explotación activa CVE-2026-105740

## Vulnerabilidad Crítica de Ejecución Remota de Código (RCE) en Langflow bajo Explotación Activa

Langflow · CWE-94: Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `Se recomienda consultar al proveedor para versiones específicas y parches.`

Actores de amenazas están explotando activamente CVE-2026-105740, una vulnerabilidad de ejecución remota de código (RCE) autenticada y crítica en Langflow, con un registro de 1,423 intentos de explotación.

**Impacto:** La explotación de esta vulnerabilidad permite a un atacante autenticado ejecutar código arbitrario en el sistema, lo que puede llevar a la pérdida de datos o al control total del sistema.

> **Acción a seguir:** Priorice la aplicación de parches de seguridad para Langflow. Refuerce las medidas de seguridad perimetral y monitoree los logs en busca de actividades sospechosas.

**Ampliar información:** NVD — CVE-2026-105740 CISA KEV

Crítica · CVSS n/d Explotación activa CVE-2026-102255

## Vulnerabilidad Crítica en SonicWall SMA 1000 Explotada Activamente

SonicWall SMA 1000 · CWE-918: Server-Side Request Forgery (SSRF) · Versiones afectadas: `Se recomienda consultar la documentación oficial de SonicWall para versiones afectadas y parches.`

La vulnerabilidad CVE-2026-102255 en SonicWall SMA 1000 permite ataques de Server-Side Request Forgery (SSRF) y la exfiltración de credenciales. Está siendo activamente explotada por actores de amenazas.

**Impacto:** La explotación permite a los atacantes acceder a recursos internos, exfiltrar información sensible como credenciales y potencialmente obtener acceso no autorizado a la red interna.

> **Acción a seguir:** Aplique inmediatamente los parches de seguridad de SonicWall para SMA 1000. Monitoree su infraestructura en busca de indicadores de compromiso (IoCs) relacionados con esta vulnerabilidad.

**Ampliar información:** NVD — CVE-2026-102255 CISA KEV

Crítica · CVSS n/d | Explotación activa | CVE-2026-110447

## Falla Crítica en Collabora Nextcloud Permite Inyección de Web Shells

Nextcloud (aplicación 'Built-in CODE Server') · CWE-94: Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: Se recomienda consultar al proveedor para versiones específicas y parches.

Una vulnerabilidad grave en la aplicación 'Built-in CODE Server' de Nextcloud (Collabora) permite a los atacantes inyectar web shells, comprometiendo los servidores. Esta vulnerabilidad está siendo activamente explotada.

**Impacto:** La inyección de web shells concede a los atacantes control persistente sobre el servidor, permitiéndoles ejecutar comandos arbitrarios, acceder a datos y escalar privilegios.

> **Acción a seguir:** Deshabilite o actualice urgentemente la aplicación 'Built-in CODE Server' en Nextcloud. Revise los sistemas en busca de la presencia de web shells y elimine cualquier artefacto malicioso.

**Ampliar información:** NVD — CVE-2026-110447 CISA KEV

Crítica · CVSS n/d | CVE-2026-99999

## Vulnerabilidad Crítica PwnEscape en Kernel Linux Permite Acceso de VMs a Memoria del Host

Kernel Linux · CWE-125: Out-of-bounds Read · Versiones afectadas: Se recomienda consultar la documentación oficial de Linux y sus distribuidores para versiones afectadas.

La vulnerabilidad PwnEscape (CVE-2026-99999) en el kernel Linux afecta tanto a máquinas virtuales (VMs) como a sus hosts, permitiendo la lectura de memoria del host desde una VM.

**Impacto:** Un atacante en una máquina virtual podría leer la memoria del sistema operativo anfitrión, lo que podría exponer información sensible, credenciales o permitir la escalada de privilegios.

> **Acción a seguir:** Parchee inmediatamente su infraestructura que utilice el kernel Linux. Mantenga sus sistemas operativos y entornos de virtualización actualizados.

**Ampliar información:** NVD — CVE-2026-99999 CISA KEV

Crítica · CVSS n/d | Sin CVE asignado

## Parche Urgente para Vulnerabilidades Críticas de RCE y DoS en Next.js

Next.js · CWE-94: Improper Control of Generation of Code ('Code Injection'); CWE-400: Uncontrolled Resource Consumption · Versiones afectadas: Todas las versiones afectadas antes del parche de emergencia.

Next.js ha publicado un parche fuera de banda para abordar dos fallas críticas de Ejecución Remota de Código (RCE) y una de Denegación de Servicio (DoS) que afectan a las aplicaciones web.

**Impacto:** La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario en los servidores afectados o causar una interrupción del servicio, comprometiendo la disponibilidad y la integridad de las aplicaciones.

> **Acción a seguir:** Aplique el parche de emergencia de Next.js inmediatamente. Verifique que todas sus aplicaciones basadas en Next.js estén actualizadas a las versiones seguras.

**Ampliar información:** Next.js: Parche Urgente para Vulnerabilidades Críticas RCE y DoS en Aplicaciones Web

Alta · CVSS 8.8 Explotación activa CVE-2026-96951

## Vulnerabilidad de Inyección de Comandos en Microsoft Windows

Microsoft Windows · CWE-77: Command Injection · Versiones afectadas: `1.0.0 – <20260925.100; 10.0.14393.0 – <10.0.14393.9612; 10.0.17763.0 – <10.0.17763.9376; 10.0.19044.0 – <10.0.19044.7…`

Microsoft Windows Shell contiene una vulnerabilidad de inyección de comandos que permite a un atacante no autorizado eludir una característica de seguridad a través de la red. Esta falla está siendo activamente explotada.

**Impacto:** Un atacante puede ejecutar comandos arbitrarios, lo que podría conducir a la toma de control del sistema o a la instalación de software malicioso.

> **Acción a seguir:** Aplique las actualizaciones de seguridad de Microsoft para Windows. CISA ha establecido un plazo para la remediación antes del 16 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-96951 CISA KEV

Alta · CVSS 8.6 Explotación activa CVE-2026-0322

## Vulnerabilidad de Inyección de Código en Palo Alto Networks PAN-OS

Palo Alto Networks PAN-OS · CWE-94: Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `12.2.0 – <12.2.4; 12.1.0 – <12.1.10-h2; 11.2.0 – <11.2.16; 11.1.0 – <11.1.16-h3; 10.2.0 – <10.2.18-h12`

Palo Alto Networks PAN-OS contiene una vulnerabilidad de inyección de código que podría permitir a un atacante autenticado con acceso a la red ejecutar código arbitrario con privilegios de root en el firewall. Esta vulnerabilidad está siendo activamente explotada.

**Impacto:** Un atacante autenticado podría obtener control total del firewall, comprometiendo la seguridad perimetral de la red y permitiendo el acceso a recursos internos.

> **Acción a seguir:** Aplique los parches de seguridad de Palo Alto Networks. El plazo de CISA para la remediación es el 17 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-0322 CISA KEV

Alta · CVSS 8.6 Explotación activa CVE-2026-104935

## Vulnerabilidad de Bypass de Autenticación por Spoofing en Ivanti Connect Secure

Ivanti Connect Secure · CWE-288: Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: `Versiones sin especificar, se recomienda consultar al proveedor.`

Ivanti Connect Secure contiene una vulnerabilidad de bypass de autenticación por spoofing que permite a un atacante remoto no autenticado ejecutar comandos arbitrarios. Esta falla está siendo activamente explotada.

**Impacto:** Un atacante puede ejecutar comandos en el sistema subyacente de Ivanti Connect Secure sin autenticación, lo que lleva a un compromiso completo del dispositivo y el acceso a la red.

> **Acción a seguir:** Aplique las actualizaciones de seguridad de Ivanti. CISA ha establecido un plazo para la remediación antes del 16 de octubre de 2026.

**Ampliar información:** NVD — CVE-2026-104935 CISA KEV

Media · CVSS 5.4 Explotación activa CVE-2025-61624

### Vulnerabilidad de Recorrido de Ruta en Fortinet Multiple Products

FortiOS, FortiPAM, FortiProxy, FortiSwitchManager · CWE-23: Relative Path Traversal · Versiones afectadas: `7.6.0 – ≤7.6.4; 7.4.0 – ≤7.4.9; 7.2.0 – ≤7.2.13; 7.0.0 – ≤7.0.19; 6.4.0 – ≤6.4.16`

FortiOS, FortiPAM, FortiProxy y FortiSwitchManager contienen una vulnerabilidad de recorrido de ruta que permite a un atacante autenticado con perfil de administrador y permisos de lectura-escritura escribir o eliminar archivos arbitrarios mediante comandos CLI específicos. Esta vulnerabilidad ha sido explotada por el malware PEERSTITCH.

**Impacto:** Un atacante autenticado puede manipular archivos críticos del sistema, lo que podría llevar a la modificación de configuraciones, denegación de servicio o, en combinación con otras vulnerabilidades, a un compromiso más profundo del sistema. El malware PEERSTITCH ha demostrado su capacidad para evadir la detección al explotar esta y otras fallas en FortiOS.

> **Acción a seguir:** Actualice sus dispositivos Fortinet (FortiOS, FortiPAM, FortiProxy, FortiSwitchManager) a las versiones que mitiguen esta vulnerabilidad. El plazo de CISA para la remediación es el 19 de octubre de 2026. Revise la documentación de Fortinet para las versiones específicas de parche.

**Ampliar información:** NVD — CVE-2025-61624 CISA KEV

## MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

### Midnight Mimosa (Malware de Proxy Residencial)

El malware 'Midnight Mimosa' se ha descubierto preinstalado en teléfonos Android de bajo costo, transformándolos en proxies residenciales. Este malware se utiliza para generar ingresos a través de fraude publicitario y otras actividades ilícitas sin el conocimiento del usuario.

MITRE ATT&CK `T1090.003 — Proxy: Multi-hop Proxy` `T1090.002 — Proxy: Domain Fronting` `T1573 — Encrypted Channel`

> **Acción a seguir:** Revise la cadena de suministro de dispositivos Android de bajo costo. Implemente soluciones EDR móvil y monitoree el tráfico de red en busca de patrones de uso inusuales que puedan indicar actividad de proxy. Eduque a los usuarios sobre los riesgos de descargar aplicaciones de fuentes no confiables.

**Ampliar información:** Malware preinstalado en Android convierte teléfonos económicos en proxies residenciales

### Hirudo (Troyano Bancario de Android)

Hirudo es un nuevo troyano bancario de Android que evade las medidas de seguridad al reemplazar aplicaciones legítimas con versiones maliciosas, lo que le permite eludir los controles de seguridad internos de las aplicaciones bancarias y robar datos financieros.

MITRE ATT&CK `T1040 — Network Sniffing` `T1056.001 — Input Capture: Keylogging` `T1115 — Clipboard Data` `T1078 — Valid Accounts` `T1143 — Network Service Scanning`

> **Acción a seguir:** Utilice soluciones de seguridad móvil que realicen análisis en tiempo real de las aplicaciones instaladas. Fomente la descarga de aplicaciones solo desde tiendas oficiales y verifique la integridad de las aplicaciones bancarias. Eduque a los usuarios sobre la detección de aplicaciones falsas.

**Ampliar información:** Hirudo: Nuevo troyano bancario de Android evade seguridad de apps legítimas

### Kits de Phishing-as-a-Service (PhaaS)

Microsoft, en colaboración con diversos partners, ha desarticulado tres kits de Phishing-as-a-Service (PhaaS) que han sido responsables de la creación y distribución de más de mil millones de mensajes fraudulentos. Estos servicios facilitan ataques de phishing a nivel global, afectando a miles de organizaciones.

MITRE ATT&CK `T1566.001 — Phishing: Spearphishing Attachment` `T1566.002 — Phishing: Spearphishing Link` `T1078 — Valid Accounts`

> **Acción a seguir:** Refuerce la autenticación multifactor (MFA) en todas las cuentas críticas. Implemente soluciones avanzadas de protección de correo electrónico y realice capacitaciones regulares a los empleados sobre cómo identificar y reportar intentos de phishing. Considere el uso de DMARC, DKIM y SPF.

**Ampliar información:** Microsoft desarticula 3 kits de phishing responsables de más de mil millones de mensajes fraudulentos

## NOTICIAS DE CIBERSEGURIDAD lo que cambia esta semana

### Agente de IA descubre bypass crítico de OTP en producción: Lecciones de seguridad web

Un agente de Inteligencia Artificial (IA) logró descubrir una vulnerabilidad crítica de bypass de la autenticación de un solo uso (OTP) en un sitio web en producción. Este incidente resalta la importancia de la validación exhaustiva de la identidad y la robustez de la seguridad de las aplicaciones, y subraya el potencial tanto ofensivo como defensivo de la IA en ciberseguridad.

**Ampliar información:** Agente de IA descubre bypass crítico de OTP en producción: Lecciones de seguridad web

ACCIÓN A SEGUIR

### Cómo te acompaña nuestro SOC

Las prioridades esta semana son aplicar los parches para las vulnerabilidades críticas de Cisco Secure Email Gateway (CVE-2026-76519) y Ahsay AhsayCBS (CVE-2026-105134) antes del 17 de octubre, así como las de Microsoft Windows (CVE-2026-96951) e Ivanti Connect Secure (CVE-2026-104935) antes del 16 de octubre. Adicionalmente, se recomienda actualizar urgentemente las plataformas afectadas por RCE activas como Bricksforge de WordPress, Langflow, SonicWall SMA 1000 y Collabora Nextcloud. Para Fortinet, se debe remediar CVE-2025-61624 antes del 19 de octubre. Mantenga una vigilancia activa sobre los dispositivos Android para detectar el malware 'Midnight Mimosa' y 'Hirudo', y refuerce las defensas contra phishing. Nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a las tácticas y técnicas de 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.