



**INGENIERÍA
TELEMÁTICA S.A.S.**

CIBERSEGURIDAD · REDES · CLOUD

● TLP: CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W39 · 21 sep 2026 – 27 sep 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta edición semanal destaca una cantidad alarmante de ocho vulnerabilidades con explotación activa, siete de ellas calificadas como Críticas y una Alta, afectando a productos ampliamente utilizados como Citrix NetScaler, WSO2, Arista VeloCloud, F5 BIG-IP APM, Check Point, Adobe Commerce/Magento y Microsoft SharePoint. Varias de estas vulnerabilidades permiten la ejecución remota de código (RCE) por parte de atacantes no autenticados. En el ámbito de las amenazas, Microsoft ha desmantelado EvilTokens, un servicio de phishing como servicio (PhaaS) impulsado por IA que comprometió miles de buzones de Office 365. Además, se ha observado que actores chinos están explotando vulnerabilidades de día cero en Chrome y Windows para desplegar el malware CLEANGULP. Es imperativo que las organizaciones prioricen la aplicación de parches y refuercen sus defensas contra estas amenazas activas para proteger sus activos críticos.

7 Crítica

1 Alta



Ciberseguridad 360°

Protección avanzada con Fortinet.



Nube Híbrida

AWS, Azure, GWorkspace, M365.



Continuidad DRP

Veeam y Acronis.



SOC Gestionado

Monitoreo y respuesta.

NIT: 816007833-0

Pereira, Colombia

+57 314 682 5259

ingenieriatelematica.com.co

Publicado 28 sep 2026

Fuentes: CISA KEV, NVD y avisos de fabricante.

[Ver detalle →](#)

VISTA RÁPIDA Severidad CVSS · explotaci3n activa (CISA KEV)

7

Crítica

1

Alta

0

Media

0

Baja

8 vulnerabilidades con explotaci3n activa confirmada · 2 campaa(s) de malware · 7 noticia(s)

VULNERABILIDADES

Crítica · CVSS 10.0

EXPLOTACI3N ACTIVA

CVE-2026-5430

WSO2 Multiple Products Path Traversal Vulnerability

WSO2 Multiple Products · · Versiones afectadas: 4.5.0 - <4.5.0.57; 4.6.0 - <4.6.0.21; 4.5.0 - <4.5.0.56; 4.5.0 - <4.5.0.58; 4.6.0 - <4.6.0.22

Vulnerabilidad de Path Traversal en mltiples productos de WSO2. La explotaci3n activa de esta falla podría permitir a un atacante acceder a directorios o archivos restringidos del sistema.

Impacto: Compromiso de la confidencialidad e integridad del sistema mediante acceso a archivos y ejecuci3n de c3digo arbitrario.

Acci3n a seguir:

Actualice sus productos WSO2 a las versiones 4.5.0.57, 4.6.0.21, 4.5.0.56, 4.5.0.58, 4.6.0.22 o superiores.
Fecha lfmite de CISA para el parcheo: 27 de septiembre de 2026.

Ampliar informaci3n: NVD — CVE-2026-5430 CISA KEV

Crítica · CVSS 10.0

EXPLOTACI3N ACTIVA

CVE-2026-93952

Arista VeloCloud Orchestrator Improper Input Validation Vulnerability

Arista VeloCloud Orchestrator · · Versiones afectadas: 5.2.0 - ≤5.2.3.15; 6.1.0 - ≤6.1.3.7; 6.4.0 - ≤6.4.2.7; 7.0.0 - ≤7.0.0.2

Arista VeloCloud Orchestrator (VCO) en sus versiones on-premise contiene una vulnerabilidad de validaci3n de entrada incorrecta. Un atacante remoto puede explotar esta falla para acceder a funcionalidades internas privilegiadas del orquestador.

Impacto: Compromiso de la confidencialidad, integridad y disponibilidad del host VCO mediante el acceso no autorizado a funcionalidades internas privilegiadas.

Acci3n a seguir:

Actualice su Arista VeloCloud Orchestrator a versiones superiores a 5.2.3.15, 6.1.3.7, 6.4.2.7 o 7.0.0.2. Fecha lfmite de CISA para el parcheo: 25 de septiembre de 2026.

Ampliar informaci3n: NVD — CVE-2026-93952 CISA KEV

Crítica · CVSS 9.8

EXPLOTACI3N ACTIVA

CVE-2026-94127

F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability

F5 BIG-IP APM · · Versiones afectadas: 21.1.0 - <Hotfix-BIGIP-21.1.0.2.0.30.22-ENG; 17.5.0 - <Hotfix-BIGIP-17.5.1.9.0.160.12-ENG; 17.1.0 - <Hotfix-BIGIP-17...

F5 BIG-IP APM presenta una vulnerabilidad de desbordamiento de bfer basado en heap cuando se configuran una poltica de acceso y un perfil OAuth en un servidor virtual. Esta falla puede ser explotada por un atacante no autenticado.

Impacto: Ejecuci3n remota de c3digo (RCE) por parte de un atacante no autenticado, lo que puede resultar en el control total del sistema afectado.

Acci3n a seguir:

Aplique el hotfix o actualice a las versiones Hotfix-BIGIP-21.1.0.2.0.30.22-ENG, Hotfix-BIGIP-17.5.1.9.0.160.12-ENG o superiores, segun corresponda a su versi3n. Fecha lfmite de CISA para el parcheo: 25 de septiembre de 2026.

Ampliar informaci3n: NVD — CVE-2026-94127 CISA KEV

Crítica · CVSS 9.8

EXPLOTACIÓN ACTIVA

CVE-2026-93616

Check Point Multiple Products Path Traversal Vulnerability

Check Point Multiple Products · · Versiones afectadas: R82.20 with no Jumbo Hotfix; R82 with Jumbo Hotfix Take 126 or below; R81 (EOS); R80.40 (EOS); R80.30 (EOS)

Los productos Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server y SmartEvent contienen una vulnerabilidad de Path Traversal. Un atacante no autenticado puede aprovechar esta falla.

Impacto: Carga y ejecución de scripts arbitrarios por un atacante no autenticado, lo que puede llevar al compromiso total de los servidores de gestión de Check Point.

Acción a seguir: Si utiliza R82.20 sin Jumbo Hotfix, o R82 con Jumbo Hotfix Take 126 o inferior, aplique las actualizaciones de seguridad más recientes. Las versiones R81, R80.40 y R80.30 han llegado al fin de soporte (EOS) y deben ser actualizadas inmediatamente. Fecha límite de CISA para el parcheo: 25 de septiembre de 2026.

Ampliar información: [NVD](#) — [CVE-2026-93616](#) [CISA KEV](#)

Crítica · CVSS 9.5

EXPLOTACIÓN ACTIVA

CVE-2026-88772

Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Citrix NetScaler · · Versiones afectadas: <14.1-73.37; <13.1-64.23; <14.1-73.37 FIPS; <13.1.37.279 FIPS and NDcPP

Citrix NetScaler ADC y NetScaler Gateway contienen una vulnerabilidad de restricción inadecuada de operaciones dentro de los límites de un búfer de memoria.

Impacto: Ejecución remota de código (RCE) o denegación de servicio (DoS) por parte de un atacante, afectando la disponibilidad y control de los dispositivos NetScaler.

Acción a seguir: Actualice sus dispositivos Citrix NetScaler a las versiones 14.1-73.37 o superiores, 13.1-64.23 o superiores, 14.1-73.37 FIPS o superiores, y 13.1.37.279 FIPS and NDcPP o superiores. Fecha límite de CISA para el parcheo: 30 de septiembre de 2026.

Ampliar información: [NVD](#) — [CVE-2026-88772](#) [CISA KEV](#)

Crítica · CVSS 9.5

EXPLOTACIÓN ACTIVA

CVE-2026-88771

Citrix NetScaler Improper Input Validation Vulnerability

Citrix NetScaler · · Versiones afectadas: <14.1-73.37; <13.1-64.23; <14.1-73.37 FIPS; <13.1.37.279 FIPS and NDcPP

Citrix NetScaler ADC y NetScaler Gateway contienen una vulnerabilidad de validación de entrada incorrecta que podría permitir a un atacante no autenticado ejecutar comandos arbitrarios.

Impacto: Ejecución remota de comandos arbitrarios por parte de un atacante no autenticado, lo que lleva a un compromiso completo del sistema.

Acción a seguir: Actualice sus dispositivos Citrix NetScaler a las versiones 14.1-73.37 o superiores, 13.1-64.23 o superiores, 14.1-73.37 FIPS o superiores, y 13.1.37.279 FIPS and NDcPP o superiores. Fecha límite de CISA para el parcheo: 30 de septiembre de 2026.

Ampliar información: [NVD](#) — [CVE-2026-88771](#) [CISA KEV](#)

Crítica · CVSS 9.1

EXPLOTACIÓN ACTIVA

CVE-2026-71362

Adobe Commerce and Magento Incorrect Authorization Vulnerability

Adobe Commerce and Magento · · Versiones afectadas: 0

Adobe Commerce y Magento contienen una vulnerabilidad de autorización incorrecta que puede ser explotada por un atacante para obtener acceso elevado a recursos sensibles sin interacción del usuario.

Impacto: Escalada de privilegios y acceso no autorizado a recursos sensibles, comprometiendo la confidencialidad e integridad de la plataforma de comercio electrónico.

Acción a seguir: Aplique los parches de seguridad más recientes disponibles para su versión de Adobe Commerce y Magento. Se asume que la versión '0' indica que todas las versiones no parcheadas son vulnerables. Fecha límite de CISA para el parcheo: 27 de septiembre de 2026.

Ampliar información: [NVD](#) — [CVE-2026-71362](#) [CISA KEV](#)

Alta · CVSS 8.8

EXPLOTACIÓN ACTIVA

CVE-2026-65660

Microsoft SharePoint Code Injection Vulnerability

Microsoft SharePoint · · Versiones afectadas: 16.0.0 - <16.0.5565.1001; 16.0.0 - <16.0.10417.20198; 16.0.0 - <16.0.19725.20522

Microsoft SharePoint presenta una vulnerabilidad de inyección de código que podría permitir a un atacante autenticado ejecutar código de forma remota a través de la red.

Impacto: Ejecución remota de código por un atacante autenticado, lo que puede llevar al control completo del servidor SharePoint y acceso a datos sensibles.

Acción a seguir: Actualice su Microsoft SharePoint a las versiones 16.0.5565.1001, 16.0.10417.20198, 16.0.19725.20522 o superiores. Fecha límite de CISA para el parcheo: 28 de septiembre de 2026.

Ampliar información: [NVD](#) — [CVE-2026-65660](#) [CISA KEV](#)

MALWARE Y CAMPAÑAS

EvilTokens PhaaS

Microsoft, junto a varios aliados, desarticuló EvilTokens, un sofisticado servicio de phishing como servicio (PhaaS) que utilizaba inteligencia artificial para comprometer cuentas de correo de Office 365. Esta campaña afectó a más de 10.000 organizaciones globalmente, comprometiendo más de 12.000 buzones.

MITRE ATT&CK: [T1566 - Phishing](#) [T1078 - Valid Accounts](#)

Acción a seguir: Implemente autenticación multifactor (MFA) robusta en todas las cuentas, especialmente las de Office 365. Eduque a los usuarios sobre las tácticas de phishing avanzadas con IA y realice simulacros regulares. Monitoree anomalías en los accesos y el comportamiento del correo electrónico.

CLEANGULP

Actores de amenaza chinos están explotando activamente vulnerabilidades de día cero en Google Chrome y Microsoft Windows para desplegar el malware CLEANGULP. Esta campaña apunta a sistemas específicos mediante la explotación de fallas no parcheadas para establecer persistencia y exfiltrar información.

MITRE ATT&CK: T1190 – Exploit Public-Facing Application T1203 – Exploitation for Client Execution
T1059 – Command and Scripting Interpreter

Acción a seguir: Mantenga sus navegadores web (especialmente Google Chrome) y sistemas operativos (Microsoft Windows) actualizados con los últimos parches de seguridad. Utilice soluciones de seguridad de endpoints (EDR) con capacidades de detección de exploits y monitoreo de comportamiento. Segmente su red para limitar el movimiento lateral en caso de compromiso.

NOTICIAS DE CIBERSEGURIDAD

Microsoft parcha vulnerabilidad crítica CVSS 10.0 en Azure AI Foundry y otros servicios

Microsoft ha publicado parches para corregir una vulnerabilidad crítica con CVSS 10.0 en Azure AI Foundry, que permitía la escalada de privilegios. Esta actualización también aborda otras vulnerabilidades en servicios de Azure, Microsoft 365 y Windows, subrayando la importancia de la gestión de parches para la seguridad en la nube y los entornos empresariales.

Alerta crítica: Explotación activa de vulnerabilidad RCE en WordPress (CVE-2026-87902)

Se ha detectado la explotación activa de una vulnerabilidad crítica de Ejecución Remota de Código (RCE), CVE-2026-87902, en WordPress. Esta falla representa un riesgo significativo para los sitios web que no han aplicado los parches correspondientes. Se recomienda la actualización urgente y la implementación de un WAF.

Día Cero 'BigDiskBuster' Bloquea Actualizaciones de Microsoft Defender: Riesgo Crítico

Un nuevo exploit de día cero, denominado 'BigDiskBuster', ha sido descubierto y está siendo utilizado para impedir que Microsoft Defender reciba actualizaciones. Esta situación deja a los endpoints desprotegidos contra las últimas amenazas, creando un riesgo crítico para la seguridad de la infraestructura.

Exploit público permite escape de contenedores a host raíz en Ubuntu Linux sin parche

Se ha hecho público un nuevo exploit que permite a atacantes escapar de contenedores y obtener acceso de host raíz en sistemas Ubuntu Linux 26.04, 24.04 y 22.04 LTS. Esta vulnerabilidad, identificada como CVE-2026-80521, reside en el kernel y requiere un parche urgente para proteger los entornos virtualizados.

CISA Alerta por Explotación Activa de Tres Vulnerabilidades Críticas en el Kernel de Linux

La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) ha emitido una alerta, añadiendo tres CVEs críticas relacionadas con el kernel de Linux a su catálogo de vulnerabilidades conocidas explotadas. Se insta a las organizaciones a aplicar parches urgentes para proteger sus sistemas contra ataques que aprovechan estas fallas.

Vulnerabilidad crítica de inyección SQL en Roundcube explotada activamente

Se ha emitido una alerta de seguridad por la explotación activa de una vulnerabilidad de inyección SQL pre-autenticación (CVE-2026-48842) en Roundcube Webmail. Esta falla crítica pone en riesgo las credenciales de los usuarios y la confidencialidad de los correos electrónicos almacenados.

Vulnerabilidad crítica RCE en Orkes Conductor explotada activamente: ¿tu empresa está protegida?

Fortinet ha alertado sobre la explotación activa de CVE-2026-58138, una vulnerabilidad crítica de Ejecución Remota de Código (RCE) pre-autenticación en Orkes Conductor. Se recomienda a las organizaciones actualizar sus sistemas, restringir el acceso o implementar un WAF para proteger su infraestructura contra esta amenaza.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Las acciones prioritarias de esta semana incluyen: 1) ****Parcheo Urgente de Vulnerabilidades Críticas (plazo 2026-09-25):**** Priorice la aplicación de parches para CVE-2026-5430 (WSO2), CVE-2026-93952 (Arista VeloCloud), CVE-2026-94127 (F5 BIG-IP APM) y CVE-2026-93616 (Check Point), cuyo plazo de aplicación de parches por CISA vence el 25 de septiembre. 2) ****Parcheo Crítico (plazo 2026-09-27/28/30):**** Continúe con el parcheo de CVE-2026-71362 (Adobe Commerce/Magento) con plazo hasta el 27 de septiembre, CVE-2026-65660 (Microsoft SharePoint) hasta el 28 de septiembre, y CVE-2026-88772 y CVE-2026-88771 (ambas de Citrix NetScaler) hasta el 30 de septiembre. 3) ****Refuerzo contra Phishing:**** Implemente o fortalezca la autenticación multifactor (MFA) en todos los servicios, especialmente Office 365, y realice campañas de concienciación sobre el phishing avanzado (EvilTokens). 4) ****Protección de Endpoints y Navegadores:**** Asegure que los navegadores web y sistemas operativos, especialmente Windows, estén actualizados para mitigar la explotación de zero-days y la distribución de malware como CLEANGULP. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a indicadores de compromiso relacionados con estas vulnerabilidades y campañas de malware 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.