INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W37 · 7 sep 2026 – 13 sep 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta semana, la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) ha emitido alertas urgentes sobre múltiples vulnerabilidades críticas que están siendo activamente explotadas. Destacan fallas de ejecución remota de código (RCE) y bypass de autenticación con CVSS 10.0 en productos de GitLab, Cisco Secure Firewall, N-able N-central y Adobe Commerce/Magento, requiriendo parches inmediatos con plazos que expiran en los próximos días. Asimismo, Citrix NetScaler presenta una vulnerabilidad crítica de bypass de autenticación bajo explotación activa. En el panorama de amenazas, se han observado campañas sofisticadas de malware como JSCeal y Gigabud, que buscan robar credenciales y evadir la detección, además de ataques de vishing dirigidos a ejecutivos para extorsión. Se recomienda a las organizaciones priorizar la aplicación de parches y fortalecer las defensas contra estas amenazas persistentes.

5 Crítica · 3 Alta

Publicado 14 sep 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)

5	3	0	0
Crítica	Alta	Media	Baja

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

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-85706

Vulnerabilidad de Path Traversal en GitLab Community Edition y Enterprise Edition

GitLab Community Edition and Enterprise Edition · CWE-22 - Path Traversal · Versiones afectadas: `18.7 - <19.1.8; 19.2 - <19.2.6; 19.3 - <19.3.2`

GitLab Community Edition y Enterprise Edition contienen una vulnerabilidad de Path Traversal que permite a un usuario no autenticado leer archivos arbitrarios debido a una inadecuada restricción de ruta y la falta de aplicación de autenticación en la API de commits del repositorio.

Impacto: Un atacante no autenticado puede leer archivos arbitrarios del sistema, lo que podría llevar a la divulgación de información sensible o a la obtención de credenciales y configuraciones, sirviendo como paso previo para ataques más complejos.

> **Acción a seguir:** Actualizar GitLab Community Edition y Enterprise Edition a las versiones 19.1.8, 19.2.6 o 19.3.2 o posteriores. La fecha límite de CISA para aplicar este parche es el 14 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-85706 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-20079

Bypass de Autenticación Crítico en Cisco Secure Firewall Management Center y Security Cloud Control

Cisco Secure Firewall Management Center (FMC) and Security Cloud Control (SCC) Firewal · CWE-288 - Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: `7.0.0; 7.0.0.1; 7.0.1; 7.1.0; 7.0.1.1`

Cisco Secure Firewall Management Center (FMC) Software y Cisco Security Cloud Control (SCC) Firewall Management contienen una vulnerabilidad de bypass de autenticación que podría permitir a un atacante remoto no autenticado eludir la autenticación y ejecutar archivos de script.

Impacto: La explotación de esta vulnerabilidad concede a un atacante remoto la capacidad de eludir la autenticación, lo que puede resultar en la ejecución de código arbitrario y el control total del dispositivo, facilitando el robo de credenciales o el despliegue de ransomware.

> **Acción a seguir:** Aplicar de inmediato los parches de seguridad proporcionados por Cisco para las versiones afectadas. La fecha límite de CISA para mitigar esta vulnerabilidad es el 12 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-20079 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-86218

Vulnerabilidad de Inyección de Código Estático en N-able N-central que Permite RCE

N-able N-central · CWE-94 - Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: <2026.3.1.14

N-able N-central contiene una vulnerabilidad de inyección de código estático que podría permitir la ejecución remota de código (RCE) con pre-autenticación.

Impacto: Un atacante podría lograr la ejecución remota de código en el sistema vulnerable sin necesidad de autenticación, lo que confiere control total sobre el servidor N-able N-central, comprometiendo la gestión de los sistemas y la infraestructura monitoreada.

> **Acción a seguir:** Actualizar N-able N-central a la versión 2026.3.1.14 o posterior. La fecha límite de CISA para aplicar este parche es el 11 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-86218 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-75650

Vulnerabilidad de Ejecución Remota de Código en Adobe Commerce y Magento Open Source (StyleSmuggler)

Adobe Commerce and Magento · CWE-917 - Improper Neutralization of Special Elements Used in a Template Engine · Versiones afectadas: 0

Adobe Commerce y Magento Open Source contienen una vulnerabilidad de neutralización inadecuada de elementos especiales utilizados en un motor de plantillas, que podría permitir a un atacante ejecutar código arbitrario.

Impacto: La explotación de esta vulnerabilidad, conocida como 'StyleSmuggler', permite a un atacante ejecutar código arbitrario en el sistema, a menudo utilizado para instalar backdoors persistentes y web shells PHP, comprometiendo completamente las tiendas online afectadas sin necesidad de autenticación.

> **Acción a seguir:** Aplicar de inmediato los parches de seguridad disponibles para Adobe Commerce y Magento Open Source. La fecha límite de CISA para la remediación es el 11 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-75650 CISA KEV

Crítica · CVSS 9.3 EXPLOTACIÓN ACTIVA CVE-2026-19490

Vulnerabilidad de Bypass de Autenticación en Citrix NetScaler ADC y NetScaler Gateway

Citrix NetScaler · CWE-288 - Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: 14.1 - ≤73.32; 13.1 - ≤63.21

Citrix NetScaler ADC y NetScaler Gateway contienen una vulnerabilidad de bypass de autenticación que involucra una ruta o canal alternativo. Cuando el dispositivo NetScaler está configurado como un servidor virtual AAA o como un Gateway (SSL VPN, ICA Proxy, CVPN o RDP Proxy), un actor de amenaza remoto no autenticado puede eludir la autenticación.

Impacto: Un atacante no autenticado puede sortear los mecanismos de autenticación, lo que puede resultar en acceso no autorizado a los recursos protegidos por Citrix NetScaler, comprometiendo la confidencialidad, integridad y disponibilidad de la red.

> **Acción a seguir:** Actualizar Citrix NetScaler ADC y NetScaler Gateway a las versiones parcheadas 14.1-73.32 y 13.1-63.21 o posteriores. La fecha límite de CISA para aplicar este parche es el 12 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-19490 CISA KEV

Alta · CVSS 8.8 EXPLOTACIÓN ACTIVA CVE-2026-87491

Vulnerabilidad de Escritura Fuera de Límites en Google Chromium V8

Google Chromium V8 · CWE-787 - Out-of-bounds Write · Versiones afectadas: `153.0.8010.36 - <153.0.8010.36`

Google Chromium V8 contiene una vulnerabilidad de escritura fuera de límites que permite a un atacante remoto ejecutar código arbitrario dentro del sandbox a través de una página HTML manipulada. Esta vulnerabilidad podría afectar a múltiples navegadores web que utilizan Chromium, incluyendo, entre otros, Google Chrome y Microsoft Edge.

Impacto: La explotación exitosa de esta vulnerabilidad permite la ejecución de código arbitrario dentro del entorno restringido del navegador. Aunque contenida por el sandbox, una cadena de exploits podría derivar en un escape del sandbox y un control total del sistema del usuario.

> **Acción a seguir:** Actualizar Google Chrome y otros navegadores basados en Chromium a la versión 153.0.8010.36 o posterior de inmediato. La fecha límite de CISA para la remediación es el 23 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-87491 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2026-85880

Desbordamiento de Búfer Basado en Heap en Microsoft Windows Advanced Local Procedure Call

Microsoft Windows · CWE-787 - Out-of-bounds Write · Versiones afectadas: `10.0.14393.0 - <10.0.14393.9512; 10.0.17763.0 - <10.0.17763.9245; 10.0.19044.0 - <10.0.19044.7725; 10.0.19045.0 - <10…`

Microsoft Windows Advanced Local Procedure Call contiene una vulnerabilidad de desbordamiento de búfer basado en heap que permite a un atacante elevar privilegios localmente.

Impacto: Un atacante local puede explotar esta vulnerabilidad para escalar sus privilegios en el sistema, obteniendo un mayor control y acceso a recursos sensibles que de otra manera estarían restringidos.

> **Acción a seguir:** Aplicar los parches de seguridad de Microsoft correspondientes a las versiones de Windows afectadas. La fecha límite de CISA para la remediación es el 22 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-85880 CISA KEV

Alta · CVSS 7.8 EXPLOTACIÓN ACTIVA CVE-2026-81963

Vulnerabilidad de Link Following en Microsoft Windows Update Stack

Microsoft Windows · CWE-59 - Improper Link Resolution Before File Access ('Link Following') · Versiones afectadas: `10.0.22631.0 - <10.0.22631.7582; 10.0.26100.0 - <10.0.26100.9445; 10.0.26200.0 - <10.0.26200.9445; 10.0.28000.0 - <10…`

Microsoft Windows Update Stack contiene una vulnerabilidad de link following que permite a un atacante local escalar privilegios hasta SYSTEM.

Impacto: Un atacante con acceso local al sistema puede aprovechar esta falla para escalar privilegios y obtener control total sobre el sistema operativo, comprometiendo la integridad y confidencialidad del mismo.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft para las versiones de Windows Update Stack afectadas. La fecha límite de CISA para la remediación es el 22 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-81963 CISA KEV

MALWARE Y CAMPAÑAS

JSCeal

JSCeal es un malware JavaScript avanzado que se especializa en el robo de cookies de sesión de Google, evadiendo la autenticación de múltiples factores (MFA). Afecta a navegadores basados en Chromium y compromete cuentas de criptomonedas, a menudo distribuido a través de campañas de malvertising.

MITRE ATT&CK: `T1539 — Session Hijacking` `T1555 — Credential Access` `T1059 — Command and Scripting Interpreter`

> **Acción a seguir:** Implementar soluciones EDR/XDR para detectar actividad anómala en navegadores y sistemas. Educar a los usuarios sobre los riesgos de malvertising y descargas de software de fuentes no confiables. Considerar el uso de Web Application Firewalls (WAF) para mitigar el acceso a scripts maliciosos.

Troyano Gigabud

El troyano bancario Gigabud ha evolucionado, ahora utiliza la creación de perfiles de trabajo falsos en dispositivos Android para ocultarse y evadir la detección por parte de aplicaciones bancarias y soluciones de seguridad móvil. Este método le permite operar de forma más sigilosa y persistente en los dispositivos comprometidos.

MITRE ATT&CK: `T1403 — Sandbox Evasion` `T1555 — Credential Access` `T1562 — Impair Defenses`

> **Acción a seguir:** Implementar soluciones de seguridad móvil (MEM) y EDR para Android que puedan detectar comportamientos anómalos y la creación de perfiles de trabajo no autorizados. Promover la descarga de aplicaciones solo desde tiendas oficiales y educar a los usuarios sobre las técnicas de ingeniería social que llevan a la instalación de malware móvil.

Web Shell en Memoria F5 BIG-IP APM

Un sofisticado malware está comprometiendo F5 BIG-IP APM inyectando un web shell directamente en la memoria (explotando CVE-2025-53521). Esta técnica le permite evadir los escaneos tradicionales basados en disco y establecer persistencia, facilitando el control remoto sin dejar rastros en el sistema de archivos.

MITRE ATT&CK: `T1505.003 — Server Software Component: Web Shell` `T1059 — Command and Scripting Interpreter` `T1562.001 — Impair Defenses: Disable or Modify Tools`

> **Acción a seguir:** Aplicar los parches de seguridad para F5 BIG-IP APM que aborden CVE-2025-53521. Implementar soluciones de detección y respuesta en endpoints (EDR) con capacidades de análisis de memoria para identificar web shells en memoria. Realizar auditorías de seguridad periódicas y monitorear la actividad de red en busca de patrones de comunicación inusuales.

NOTICIAS DE CIBERSEGURIDAD

Ataques de Vishing a ejecutivos roban datos de Microsoft 365 para extorsión

Se ha detectado una serie de ataques de vishing (phishing de voz) dirigidos a ejecutivos, donde los atacantes suplantan a personal de soporte de TI. El objetivo es robar credenciales de Microsoft 365, a menudo utilizando técnicas de robo de tokens Adversary-in-the-Middle (AitM) para eludir la autenticación multifactor (MFA), con el fin de extorsionar a las víctimas.

Vulnerabilidad crítica en VMware Workstation y Fusion permite ejecutar código en el host

Broadcom ha corregido fallas críticas (CVE-2026-59346 y CVE-2026-59347) en VMware Workstation y Fusion. Estas vulnerabilidades permiten que atacantes locales ejecuten código arbitrario en el sistema host desde una máquina virtual, comprometiendo la seguridad del entorno virtualizado. Se insta a los usuarios a aplicar los parches con urgencia.

SAP corrige vulnerabilidad crítica CVSS 10.0 que permite RCE no autenticado

SAP ha lanzado parches para abordar múltiples fallas de seguridad de máxima gravedad, incluyendo una vulnerabilidad crítica con CVSS 10.0 que permite la ejecución remota de código sin autenticación en el kernel. Esta falla representa un riesgo significativo para la integridad y disponibilidad de los sistemas SAP, por lo que se recomienda la aplicación inmediata de las actualizaciones.

Exploit público para vulnerabilidades RCE en Telerik UI (ASP.NET AJAX): parche urgente

Se ha liberado un exploit público que afecta a Telerik UI para ASP.NET AJAX, permitiendo la ejecución remota de código (RCE) no autenticada en sistemas con configuraciones específicas. Esta situación eleva el riesgo de compromiso para las aplicaciones que utilizan esta librería, haciendo que la actualización sea una prioridad crítica para prevenir ataques.

Check Point parcha vulnerabilidades críticas en VPN: riesgo de ejecución remota de código (RCE)

Check Point ha corregido dos fallas críticas (CVSS 9.8) en sus productos Security Gateway y Security Management Server. Estas vulnerabilidades podrían permitir la ejecución remota de código no autenticado a través de conexiones VPN. Se han lanzado parches para mitigar estos riesgos significativos, que podrían exponer la infraestructura a ataques directos.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorizar la aplicación de parches para las vulnerabilidades críticas con explotación activa, especialmente CVE-2026-85706 (GitLab), CVE-2026-20079 (Cisco FMC), CVE-2026-86218 (N-able N-central), y CVE-2026-75650 (Adobe Commerce/Magento), dado su CVSS de 10.0 y plazos de CISA inminentes (11-14 de septiembre). Posteriormente, abordar CVE-2026-19490 (Citrix NetScaler) y CVE-2026-87491 (Google Chrome), así como las vulnerabilidades de elevación de privilegios en Microsoft Windows. Fortalecer las defensas contra ataques de vishing mediante concienciación y soluciones de seguridad de identidad. Desplegar controles para detectar y mitigar malware como JSCeal, Gigabud y la inyección de web shells en memoria en F5 BIG-IP APM. Nuestro monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a las tácticas, técnicas y procedimientos (TTPs) asociados a estas amenazas para proteger su infraestructura.