INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W26 · 22 jun 2026 – 28 jun 2026

Boletín de Ciberseguridad

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

RESUMEN EJECUTIVO

Esta semana, el Boletín de Ciberseguridad destaca la urgencia de parchear múltiples vulnerabilidades críticas y de alta severidad, varias de ellas con explotación activa y plazos de mitigación inminentes por parte de CISA. En particular, tres vulnerabilidades críticas (CVSS 10.0) que afectan a Ubiquiti UniFi OS, una inyección de código crítica (CVSS 9.8) en Lantronix EDS5000, y una vulnerabilidad crítica de validación de entrada (CVSS 9.3) en PTC Windchill y FlexPLM, todas con fecha límite de remediación el 26 de junio de 2026. También se reporta una vulnerabilidad de alta severidad (CVSS 8.6) en Cisco Unified Communications Manager con plazo hasta el 28 de junio. Adicionalmente, se ha identificado la campaña 'FortiBleed', que compromete miles de dispositivos FortiGate globalmente mediante el uso de credenciales débiles y la ausencia de MFA, subrayando la importancia de una gestión robusta de credenciales y la implementación de autenticación multifactor. Las amenazas de malware de la semana incluyen el ransomware DragonForce, el clipper CryptoBandits, el backdoor STOCKSTAY de Turla, y el troyano bancario Rokarolla, entre otros, destacando la evolución en técnicas de evasión y ataque a la cadena de suministro.

5 Crítica · 1 Alta

Publicado 29 jun 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	1	0	0
Crítica	Alta	Media	Baja

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

VULNERABILIDADES

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-34910

Ubiquiti UniFi OS Improper Input Validation Vulnerability

Ubiquiti UniFi OS · CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') · Versiones afectadas: `<5.0.8; <5.1.12; <5.1.11`

Esta vulnerabilidad en Ubiquiti UniFi OS se debe a una validación de entrada inadecuada que permite a un atacante con acceso a la red realizar inyección de comandos. La explotación puede llevar a la ejecución de comandos arbitrarios con privilegios elevados en el sistema subyacente.

Impacto: Un actor malicioso con acceso a la red puede lograr la ejecución remota de comandos, comprometiendo completamente el sistema y potencialmente afectando la confidencialidad, integridad y disponibilidad de la infraestructura de red gestionada por UniFi OS.

> **Acción a seguir:** Es imperativo actualizar las versiones de Ubiquiti UniFi OS a la brevedad posible. Se recomienda actualizar a versiones 5.0.8 o superior, 5.1.12 o superior, o 5.1.11 o superior para mitigar esta vulnerabilidad. La fecha límite para esta mitigación es el 26 de junio de 2026.

Ampliar información: NVD — CVE-2026-34910 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-34909

Ubiquiti UniFi OS Path Traversal Vulnerability

Ubiquiti UniFi OS · CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') · Versiones afectadas: `<5.0.8; <4.0.14; <5.1.12`

Ubiquiti UniFi OS contiene una vulnerabilidad de Path Traversal que, si es explotada, permite a un actor malicioso con acceso a la red acceder a archivos sensibles en el sistema subyacente. Estos archivos podrían ser manipulados para obtener acceso a una cuenta interna.

Impacto: La explotación de esta vulnerabilidad podría permitir a un atacante acceder y manipular archivos críticos del sistema, llevando a una escalada de privilegios o al compromiso de cuentas de usuario, resultando en acceso no autorizado y posible control del sistema.

> **Acción a seguir:** Se debe actualizar Ubiquiti UniFi OS a una versión que mitigue esta vulnerabilidad. Asegúrese de que sus sistemas estén actualizados a versiones 5.0.8 o superior, 4.0.14 o superior, o 5.1.12 o superior. La fecha límite para esta mitigación es el 26 de junio de 2026.

Ampliar información: NVD — CVE-2026-34909 CISA KEV

Crítica · CVSS 10.0 EXPLOTACIÓN ACTIVA CVE-2026-34908

Ubiquiti UniFi OS Improper Access Control Vulnerability

Ubiquiti UniFi OS · CWE-284: Improper Access Control · Versiones afectadas: <5.0.8; <5.1.12; <5.1.11

Una vulnerabilidad de control de acceso inadecuado en Ubiquiti UniFi OS podría permitir a un actor malicioso con acceso a la red realizar cambios no autorizados en la configuración y operación del sistema.

Impacto: Esta falla puede ser utilizada por un atacante para alterar la configuración del sistema, crear usuarios no autorizados, o deshabilitar funcionalidades de seguridad, comprometiendo la integridad y la disponibilidad del servicio y la red gestionada.

> **Acción a seguir:** Es crucial actualizar las versiones de Ubiquiti UniFi OS afectadas. Se recomienda encarecidamente actualizar a versiones 5.0.8 o superior, 5.1.12 o superior, o 5.1.11 o superior. La fecha límite para esta mitigación es el 26 de junio de 2026.

Ampliar información: NVD — CVE-2026-34908 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2025-67038

Lantronix EDS5000 Code Injection Vulnerability

Lantronix EDS5000 · CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') · Versiones afectadas: N/A

Lantronix EDS5000 es vulnerable a una inyección de código que permite a los atacantes insertar comandos arbitrarios del sistema operativo en el parámetro de nombre de usuario. Estos comandos son ejecutados con privilegios de root.

Impacto: La ejecución de comandos con privilegios de root otorga al atacante control total sobre el dispositivo Lantronix EDS5000, permitiendo la exfiltración de datos, la instalación de malware persistente o la interrupción de servicios críticos.

> **Acción a seguir:** Se requiere una acción inmediata para mitigar esta vulnerabilidad. Aunque no se especifican versiones, es crucial aplicar cualquier parche o actualización proporcionado por el fabricante. La fecha límite para esta mitigación es el 26 de junio de 2026.

Ampliar información: NVD — CVE-2025-67038 CISA KEV

Crítica · CVSS 9.3 EXPLOTACIÓN ACTIVA CVE-2026-12569

PTC Windchill and FlexPLM Improper Input Validation Vulnerability

PTC Windchill and FlexPLM · CWE-20: Improper Input Validation · Versiones afectadas: ≤11.0 M030; 11.1 M020; 11.2.1.0; 12.0.2.0; 12.1.2.0

PTC Windchill y FlexPLM presentan una vulnerabilidad de validación de entrada inadecuada que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario enviando una solicitud maliciosa a la red.

Impacto: La explotación exitosa de esta vulnerabilidad resulta en la ejecución remota de código arbitrario, lo que podría llevar al control completo de los sistemas afectados, el robo de datos sensibles o la interrupción de las operaciones comerciales.

> **Acción a seguir:** Es imperativo aplicar las actualizaciones de seguridad para PTC Windchill y FlexPLM. Los administradores deben asegurar que las versiones sean superiores a las indicadas: 11.0 M030, 11.1 M020, 11.2.1.0, 12.0.2.0 y 12.1.2.0. La fecha límite para esta mitigación es el 28 de junio de 2026.

Ampliar información: NVD — CVE-2026-12569 CISA KEV

Alta · CVSS 8.6 EXPLOTACIÓN ACTIVA CVE-2026-20230

Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability

Cisco Unified Communications Manager · CWE-918: Server-Side Request Forgery (SSRF) · Versiones afectadas: N/A

Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME) contienen una vulnerabilidad de Server-Side Request Forgery (SSRF) que podría permitir a un atacante remoto no autenticado escribir archivos en el sistema operativo subyacente.

Impacto: Un atacante no autenticado podría explotar esta vulnerabilidad para escribir archivos en el sistema, lo que podría conducir a una escalada de privilegios, la ejecución de código arbitrario o la interrupción de los servicios de comunicaciones.

> **Acción a seguir:** Se recomienda aplicar las actualizaciones o parches de seguridad de Cisco tan pronto como estén disponibles para Cisco Unified Communications Manager y Unified CM SME. La fecha límite para esta mitigación es el 28 de junio de 2026.

Ampliar información: NVD — CVE-2026-20230 CISA KEV

MALWARE Y CAMPAÑAS

FortiBleed + explotación de FortiSandbox (Fortinet)

Dos frentes de ataque convergen sobre la infraestructura Fortinet esta semana. La campaña 'FortiBleed' ha comprometido más de 86,000 dispositivos FortiGate a nivel global —incluyendo Colombia— aprovechando credenciales débiles, antiguas y la ausencia de Autenticación Multifactor (MFA). En paralelo, se reporta la explotación de tres vulnerabilidades críticas en Fortinet FortiSandbox. En conjunto, elevan el riesgo de toda la superficie Fortinet expuesta a Internet. Fortinet y CISA han emitido alertas y recomendaciones urgentes.

MITRE ATT&CK: `T1078 — Valid Accounts` `T1110 — Brute Force` `T1190 — Exploit Public-Facing Application` `T1552.001 — Credentials in Files`

> **Acción a seguir:** Implementar MFA en todos los dispositivos FortiGate expuestos a Internet y forzar el cambio de credenciales débiles o antiguas. Aplicar sin demora los parches de FortiSandbox para las vulnerabilidades en explotación. Auditar los registros de acceso en busca de actividad sospechosa y eliminar cuentas por defecto o en desuso.

DragonForce Ransomware (Backdoor.Turn)

El grupo DragonForce emplea el Backdoor.Turn para camuflar su tráfico de comando y control (C2) dentro de los relevos legítimos de Microsoft Teams. Utilizan técnicas avanzadas como BYOVD (Bring Your Own Vulnerable Driver) para evadir la detección y mantener la persistencia en las redes corporativas.

MITRE ATT&CK: `T1071.001 — Application Layer Protocol: Web Protocols` `T1105 — Ingress Tool Transfer` `T1059 — Command and Scripting Interpreter`

> **Acción a seguir:** Implementar un monitoreo de red robusto para detectar anomalías en el tráfico de Microsoft Teams. Restringir la ejecución de drivers no firmados o no aprobados. Mantener los sistemas operativos y software actualizados. Educar a los usuarios sobre tácticas de ingeniería social que podrían llevar a la instalación inicial del backdoor.

Clipper CryptoBandits

Microsoft ha documentado una campaña de malware denominada CryptoBandits que se propaga a través de unidades USB comprometidas y utiliza la red Tor para su comunicación de comando y control. El malware está diseñado para robar criptomonedas y datos sensibles del portapapeles en sistemas Windows.

MITRE ATT&CK: `T1564.001 — Hide Artifacts: Hidden Files and Directories` `T1552.001 — Credential Access: Credentials In Files`

> **Acción a seguir:** Deshabilitar la ejecución automática de medios extraíbles (AutoRun). Implementar políticas de control de dispositivos para restringir el uso de unidades USB no autorizadas. Utilizar soluciones de seguridad de endpoints con capacidades de detección de malware basado en comportamiento y mantenerlas actualizadas. Educar a los usuarios sobre los riesgos de conectar dispositivos USB desconocidos.

STOCKSTAY (Grupo Turla)

Google ha revelado detalles sobre STOCKSTAY, un nuevo backdoor basado en .NET desplegado por el grupo de ciberespionaje Turla. Este malware está siendo utilizado en ataques dirigidos contra entidades gubernamentales y militares en Ucrania y Europa, con el objetivo de exfiltrar información sensible.

MITRE ATT&CK: `T1071 — Application Layer Protocol` `T1021 — Remote Services` `T1105 — Ingress Tool Transfer` `T1560 — Archive Collected Data`

> **Acción a seguir:** Fortalecer la seguridad de endpoints y redes con soluciones EDR/XDR capaces de detectar comportamientos anómalos. Implementar segmentación de red para limitar el movimiento lateral. Realizar análisis de logs para identificar comunicaciones C2 sospechosas. Aplicar parches de seguridad de manera oportuna para cerrar posibles vectores de infección.

NarwhalRAT (Grupo APT37/ScarCruft)

El grupo norcoreano APT37 (también conocido como ScarCruft) está utilizando alertas falsas de seguridad de Microsoft como vector inicial para desplegar NarwhalRAT. Este malware sofisticado está diseñado para el robo de datos, empleando técnicas avanzadas de phishing para engañar a las víctimas.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1204.002 — User Execution: Malicious File` `T1059 — Command and Scripting Interpreter`

> **Acción a seguir:** Fortalecer los controles de correo electrónico con filtros anti-phishing avanzados. Capacitar a los empleados para reconocer correos electrónicos y alertas falsas. Deshabilitar macros en documentos de Office por defecto. Implementar un EDR/XDR para detectar y bloquear la ejecución de payloads maliciosos.

Phishing 'Photo ZIP' (TonRAT)

Microsoft ha alertado sobre una campaña de phishing 'Photo ZIP' dirigida a la industria hotelera. Los atacantes utilizan Node.js y técnicas de 'authentication laundering' para implantar el malware TonRAT, buscando obtener acceso persistente a los sistemas de las víctimas.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1059.006 — Command and Scripting Interpreter: Node.js` `T1105 — Ingress Tool Transfer`

> **Acción a seguir:** Reforzar la seguridad del correo electrónico con soluciones anti-phishing que detecten URL maliciosas y adjuntos sospechosos. Implementar políticas de acceso a la web y control de aplicaciones. Capacitar al personal para identificar y reportar intentos de phishing, especialmente aquellos con características de 'authentication laundering'.

Miasma

El malware Miasma ha evolucionado para realizar ataques a la cadena de suministro, comprometiendo paquetes npm y flujos de GitHub Actions. Su objetivo principal es robar credenciales de desarrolladores, lo que representa un riesgo significativo para la integridad del código y los procesos de desarrollo.

MITRE ATT&CK: `T1195.002 — Supply Chain Compromise: Compromise Software Dependencies and Development Tools` `T1552.001 — Credential Access: Credentials in Files` `T1059 — Command and Scripting Interpreter`

> **Acción a seguir:** Implementar revisiones de seguridad para todos los paquetes npm y dependencias de código. Utilizar herramientas de escaneo de seguridad en el CI/CD para identificar código malicioso. Aplicar MFA a todas las cuentas de desarrollador y servicios de integración continua. Monitorear los logs de GitHub Actions para detectar actividades anómalas.

Rokarolla

Rokarolla es un nuevo troyano bancario Android altamente sofisticado que tiene la capacidad de tomar el control total de los dispositivos móviles. Está diseñado para robar PINs, códigos SMS de doble factor y fondos de criptomonedas, comprometiendo gravemente la seguridad financiera de las víctimas.

MITRE ATT&CK: `T1056.001 — Input Capture: Keylogging` `T1111 — Multi-Factor Authentication Interception` `T1213 — Data from Local System`

> **Acción a seguir:** Educar a los usuarios sobre la descarga de aplicaciones solo de fuentes oficiales y la verificación de permisos. Utilizar soluciones de seguridad móvil para la detección de malware. No hacer clic en enlaces sospechosos ni abrir archivos adjuntos de remitentes desconocidos en dispositivos móviles. Mantener el sistema operativo Android actualizado.

NOTICIAS DE CIBERSEGURIDAD

Vulnerabilidad en SDK de Google Vertex AI: Secuestro de Modelos por 'Bucket Squatting'

Una falla conocida como 'Pickle in the Middle' en el SDK de Google Vertex AI permitió el secuestro de modelos de Machine Learning (ML) y la ejecución de código malicioso mediante 'Bucket Squatting'. Se enfatiza la importancia de mantener actualizado el SDK para mitigar este riesgo.

AutoJack: Ataque que Secuestra Agentes de IA para Ejecución Remota de Código

El exploit AutoJack permite la ejecución de código arbitrario secuestrando agentes de Inteligencia Artificial (IA), como AutoGen Studio de Microsoft. Esta técnica subraya los riesgos de seguridad emergentes en el desarrollo y uso de IA, y la necesidad de implementar medidas de protección adecuadas.

Explotación de Zero-Day en Cisco Catalyst SD-WAN Permite Acceso Root

Se ha confirmado la explotación de una vulnerabilidad zero-day (CVE-2026-20245) en Cisco Catalyst SD-WAN, que permite a los atacantes obtener acceso root. Esta explotación resalta la importancia de monitorear las alertas de seguridad de los fabricantes y aplicar las mitigaciones con prontitud.

Exploit 'usbliter8' unparcheable en chips Apple A12 y A13: Riesgo persistente para la seguridad física

Se ha descubierto 'usbliter8', un exploit de hardware unparcheable que afecta los chips Apple A12 y A13. Requiere acceso físico al dispositivo y representa un riesgo persistente para la seguridad de los dispositivos vulnerables, destacando la importancia de la seguridad física.

Microsoft Defender: nueva vulnerabilidad Zero-Day 'RoguePlanet' de escalada de privilegios

Microsoft ha confirmado una vulnerabilidad zero-day en Defender (CVE-2026-50656), conocida como 'RoguePlanet', que permite la escalada de privilegios. Aunque se espera un parche, la falla afecta la protección en tiempo real, lo que requiere atención a otras capas de seguridad.

Vulnerabilidades Críticas en NGINX Open Source: Parches Urgentes para Ejecución Remota de Código (RCE)

F5 ha lanzado parches críticos para dos fallas en NGINX Open Source (CVE-2026-42530, CVE-2026-42055) que permiten la Ejecución Remota de Código (RCE). Es fundamental actualizar de inmediato NGINX para proteger la infraestructura y evitar compromisos de seguridad.

INTERPOL alerta: Aumento de Phishing, Ransomware y Estafas con IA en ciberdelincuencia global

Un informe de INTERPOL revela un dramático incremento de ciberataques a nivel global, incluyendo phishing, ransomware y fraudes potenciados por inteligencia artificial (IA). Este panorama exige que las organizaciones refuercen sus defensas y estrategias de ciberseguridad.

Falla crítica 'One-Click' en Microsoft 365 Copilot permitía robo de datos y códigos MFA

Una vulnerabilidad de 'un solo clic' en Microsoft 365 Copilot Enterprise Search permitía la exfiltración de correos electrónicos, archivos y códigos de Autenticación Multifactor (MFA). Es crucial estar al tanto de las mitigaciones para proteger la información corporativa sensible.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Las acciones prioritarias de esta semana incluyen: 1. Aplicar de inmediato los parches para las vulnerabilidades críticas de Ubiquiti UniFi OS (CVE-2026-34910, -34909, -34908) y Lantronix EDS5000 (CVE-2025-67038) antes del 26 de junio de 2026. 2. Parchear PTC Windchill y FlexPLM (CVE-2026-12569) y Cisco Unified Communications Manager (CVE-2026-20230) antes del 28 de junio de 2026. 3. Fortalecer las defensas contra la campaña 'FortiBleed' implementando MFA y rotando credenciales en todos los dispositivos FortiGate. 4. Reforzar la seguridad de correo electrónico, endpoint y redes para mitigar riesgos de campañas de malware como DragonForce, CryptoBandits, STOCKSTAY, NarwhalRAT, Photo ZIP, Miasma y Rokarolla. Nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está disponible para ayudar a su organización a detectar y mitigar proactivamente estas amenazas.