INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W38 · SEMANAL

Semana del 14 sep 2026 al 20 sep 2026 · publicado el 21 de septiembre 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

La edición semanal del Boletín de Ciberseguridad destaca un conjunto de vulnerabilidades críticas y de alta severidad con explotación activa, particularmente afectando productos de Cisco y el Kernel de Linux, que requieren atención inmediata. Adicionalmente, se reportan campañas de malware sofisticadas como RatHat para Android, BambooToken para sistemas Windows y Linux, y el backdoor SparroWocky del grupo FamousSparrow, con un enfoque geográfico en Latinoamérica. El desmantelamiento del servicio DDoS NightmareStresser y alertas sobre ataques avanzados de phishing a cuentas de Microsoft Cloud completan el panorama de amenazas de esta semana.

7	7	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

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

7 vulnerabilidades, 7 con explotación activa confirmada · 3 campaña(s) de malware · 3 noticia(s) · semana del 14 sep 2026 al 20 sep 2026

VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 10.0 | Explotación activa | CVE-2026-76460

Falla de Uso Incorrecto de APIs Privilegiadas en Cisco Identity Services Engine

Cisco Identity Services Engine · CWE-285 · Versiones afectadas: `3.1.0 p8; 3.1.0 p9; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3`

Una vulnerabilidad de uso incorrecto de APIs privilegiadas en Cisco Identity Services Engine (ISE) y Cisco ISE Passive Identity Connector (ISE-PIC) podría permitir a un atacante remoto no autenticado obtener acceso no autorizado al dispositivo afectado, al eludir la interfaz de gestión web.

Impacto: Acceso no autorizado y posible control total del dispositivo sin necesidad de autenticación, comprometiendo gravemente la seguridad de la red y la infraestructura de identidad.

> **Acción a seguir:** Actualice Cisco Identity Services Engine a las versiones parcheadas. Se recomienda aplicar esta mitigación antes del 19 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-76460 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2025-39682

Falla de Verificación Impropia de Condiciones en el Kernel de Linux (TLS)

Linux Kernel · CWE-703 · Versiones afectadas: `84c61fe1a75b4255df1e1e7c054c9e6d048da417 - <2902c3ebcca52ca845c03182000e8d71d3a5196f; 84c61fe1a75b4255df1e1e7c054c9e6…`

El Kernel de Linux contiene una vulnerabilidad de verificación impropia de condiciones inusuales o excepcionales en la ruta de recepción de TLS. Esto permite que un registro de longitud cero, recuperado de la lista rx_list, eluda el manejo previsto del tipo de registro recvmsg(), lo que podría causar que los registros TLS posteriores se procesen incorrectamente.

Impacto: La manipulación de registros TLS puede conducir a la denegación de servicio, corrupción de datos o, potencialmente, a la ejecución remota de código, afectando la confidencialidad, integridad y disponibilidad de las comunicaciones.

> **Acción a seguir:** Aplique los parches disponibles para el Kernel de Linux que abordan esta vulnerabilidad. Se recomienda aplicar esta mitigación antes del 21 de septiembre de 2026.

Ampliar información: NVD — CVE-2025-39682 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-76461

Vulnerabilidad de Inyección SQL en Cisco Secure Email Gateway

Cisco Secure Email Gateway · CWE-89 · Versiones afectadas: `14.0.0-698; 13.5.1-277; 13.0.0-392; 14.2.0-620; 13.0.5-007`

El software AsyncOS para Cisco Secure Email Gateway (SEG) contiene una vulnerabilidad de inyección SQL que podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios con privilegios de root en el sistema operativo subyacente.

Impacto: Un atacante puede obtener control total sobre el sistema operativo del gateway, incluyendo la ejecución de comandos con privilegios de root, lo que resulta en una exposición completa de datos sensibles, interrupción del servicio o el uso del sistema como punto de pivote para ataques adicionales.

> **Acción a seguir:** Actualice Cisco AsyncOS para Cisco Secure Email Gateway a las versiones parcheadas. Se recomienda aplicar esta mitigación antes del 17 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-76461 CISA KEV

Alta · CVSS 8.8 **Explotación activa** CVE-2026-53266

Escritura Fuera de Límites en el Kernel de Linux (ebtables SNAT)

Linux Kernel · CWE-787 · Versiones afectadas: `63137bc5882a1882c553d389fdeeeace86ee1741 - <bf84ad7c7a9ede46e31afaa41a1ba06a159e8c87; 63137bc5882a1882c553d389fdeeeac…`

El Kernel de Linux contiene una vulnerabilidad de escritura fuera de límites en el objetivo ebtables SNAT, permitiendo que una reescritura de dirección de hardware de remitente ARP escriba directamente en un fragmento de búfer de socket no lineal respaldado por una página de archivo importada por splice.

Impacto: La explotación de esta vulnerabilidad puede conducir a la corrupción de la memoria, escalada de privilegios o la ejecución de código arbitrario, comprometiendo la estabilidad y seguridad del sistema operativo.

> **Acción a seguir:** Aplique los parches de seguridad para el Kernel de Linux que corrigen esta vulnerabilidad. Se recomienda aplicar esta mitigación antes del 21 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-53266 CISA KEV

Alta · CVSS 8.8 **Explotación activa** CVE-2026-58704

Autorización Impropia en Dispositivos Google Pixel (Módem Celular)

Google Pixel · CWE-285 · Versiones afectadas: `Android kernel`

Los dispositivos Google Pixel contienen una vulnerabilidad de autorización impropia en el módem celular. Un error lógico puede permitir a un atacante eludir las comprobaciones de permisos y escalar privilegios en el dispositivo.

Impacto: Un atacante podría obtener la escalada de privilegios, obteniendo acceso y control sobre funciones y datos sensibles del dispositivo móvil que de otro modo estarían protegidos.

> **Acción a seguir:** Aplique las actualizaciones de seguridad disponibles para los dispositivos Google Pixel, que incluyen parches para el kernel de Android. Se recomienda aplicar esta mitigación antes del 19 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-58704 CISA KEV

Alta · CVSS 7.8 **Explotación activa** CVE-2025-39964

Condición de Carrera en el Kernel de Linux (Sockets AF_ALG)

Linux Kernel · CWE-362 · Versiones afectadas: `8ff590903d5fc7f5a0a988c38267a3d08e6393a2 - <0f28c4adbc4a97437874c9b669fd7958a8c6d6ce; 8ff590903d5fc7f5a0a988c38267a3d…`

El Kernel de Linux contiene una vulnerabilidad de condición de carrera que permite escrituras concurrentes al mismo socket AF_ALG. Esto causa que los datos se entrelacen de forma impredecible y se creen inconsistencias en el estado interno del socket.

Impacto: Una condición de carrera puede llevar a la corrupción de datos, denegación de servicio o, en casos avanzados, a la ejecución de código arbitrario debido al estado inconsistente del socket.

> **Acción a seguir:** Implemente las actualizaciones de seguridad del Kernel de Linux que resuelven esta condición de carrera. Se recomienda aplicar esta mitigación antes del 21 de septiembre de 2026.

Ampliar información: NVD — CVE-2025-39964 CISA KEV

Baja · CVSS n/d | Explotación activa | CVE-2026-87886

Permisos Predeterminados Incorrectos en Acronis Backup

Acronis Backup · CWE-732 · Versiones afectadas: -

Acronis Backup presenta una vulnerabilidad de permisos predeterminados incorrectos. Aunque CISA KEV no asigna un puntaje CVSS, Acronis ha alertado que esta falla permite la escalada de privilegios y está siendo explotada activamente en ataques dirigidos, especialmente en su plugin para cPanel y WHM, siendo considerada 'Crítica' por el proveedor.

Impacto: Un atacante con acceso inicial podría escalar sus privilegios en el sistema afectado, obteniendo un control más elevado sobre la copia de seguridad y los datos gestionados, comprometiendo la integridad y confidencialidad de la información.

> **Acción a seguir:** Actualice Acronis Backup, especialmente el plugin para cPanel y WHM, a las versiones que corrijan los permisos predeterminados incorrectos. Se recomienda aplicar esta mitigación antes del 19 de septiembre de 2026.

Ampliar información: NVD — CVE-2026-87886 CISA KEV

MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

RatHat (Android Malware)

RatHat es un sofisticado malware Android de origen chino que abusa de Android Debug Bridge (ADB) y utiliza técnicas avanzadas, incluyendo la asistencia de IA, para persistir en los dispositivos incluso después de una desinstalación aparente. Permite a los actores de amenazas controlar remotamente los dispositivos afectados, eludiendo la detección y comprometiendo la privacidad del usuario.

MITRE ATT&CK: `T1219 — Remote Access Software` `T1059 — Command and Scripting Interpreter` `T1574 — Hijack Execution Flow` `T1098 — Account Manipulation` `T1114 — Email Collection`

> **Acción a seguir:** Implemente soluciones de seguridad móvil (MDM/EMM con capacidades de EDR) para monitorear y bloquear actividades inusuales. Capacite a los usuarios sobre los riesgos de instalar aplicaciones de fuentes no oficiales y de habilitar ADB sin supervisión. Realice análisis periódicos de comportamiento en dispositivos Android corporativos.

Ampliar información: Malware RatHat para Android Abusa de ADB y Persiste tras Desinstalación con IA

BambooToken (Windows/Linux Malware)

BambooToken es un malware multiplataforma que utiliza el protocolo MQTT para establecer canales de comando y control (C2) sobre sistemas Windows y Linux. Ha sido observado en ataques dirigidos a entidades en Sudamérica, empleando técnicas como DLL sideloading para su ejecución y persistencia, lo que dificulta su detección.

MITRE ATT&CK: `T1071.002 — Application Layer Protocol: External Remote Services (MQTT)` `T1574.002 — DLL Search-Order Hijacking` `T1053 — Scheduled Task/Job` `T1059 — Command and Scripting Interpreter` `T1082 — System Information Discovery`

> **Acción a seguir:** Monitoree el tráfico de red en busca de comunicaciones MQTT inusuales. Implemente EDR para detectar DLL sideloading y otras técnicas de ejecución. Mantenga los sistemas operativos y software actualizados. Bloquee indicadores de compromiso conocidos y realice análisis de vulnerabilidades para identificar configuraciones débiles en su infraestructura.

Ampliar información: Malware BambooToken usa MQTT para controlar sistemas Windows y Linux en ataques a Sudamérica

SparroWocky (Backdoor de FamousSparrow)

El grupo de amenazas persistentes avanzadas (APT) FamousSparrow, alineado con intereses chinos, está desplegando el sofisticado backdoor SparroWocky contra entidades gubernamentales en Latinoamérica. Este malware está diseñado para el acceso persistente, la exfiltración de información y el establecimiento de canales de comando y control encubiertos.

MITRE ATT&CK `T1071 — Application Layer Protocol` `T1090 — Proxy` `T1059 — Command and Scripting Interpreter` `T1547 — Boot or Logon Autostart Execution` `T1082 — System Information Discovery` `T1003 — OS Credential Dumping`

> **Acción a seguir:** Refuerce la detección de intrusiones y los controles de acceso. Implemente soluciones EDR y XDR que detecten comportamientos anómalos y actividades de backdoor. Monitoree de cerca la actividad en servidores y endpoints gubernamentales, prestando especial atención a la actividad de red hacia destinos inusuales y la exfiltración de datos.

Ampliar información: China-Aligned FamousSparrow Despliega Backdoor SparroWocky en Latinoamérica

NOTICIAS DE CIBERSEGURIDAD lo que cambia esta semana

Falla crítica en Unbound DNSSEC (CVE-2026-81642) habilita RCE y DoS

Una vulnerabilidad crítica (CVE-2026-81642) ha sido identificada en Unbound DNSSEC, un validador de DNS ampliamente utilizado. Esta falla permite la ejecución remota de código (RCE) y la denegación de servicio (DoS) por parte de un atacante remoto, lo que podría comprometer seriamente la resolución de nombres en su red. Se recomienda a los usuarios de Unbound actualizar sus sistemas de inmediato.

Ampliar información: Falla crítica en Unbound DNSSEC (CVE-2026-81642) habilita RCE y DoS

Desmantelado NightmareStresser: Autoridades incautan dominios de servicio DDoS por encargo

Las autoridades internacionales han logrado desmantelar NightmareStresser, un conocido servicio de 'DDoS por encargo', incautando sus dominios y deteniendo sus operaciones. Esta acción es un golpe significativo contra la infraestructura de ciberdelincuencia que facilitaba ataques de denegación de servicio a escala. Aunque el servicio fue desmantelado, se recomienda a las organizaciones fortalecer sus defensas contra DDoS y estar atentas a la aparición de nuevos servicios similares.

Ampliar información: Desmantelado NightmareStresser: Autoridades incautan dominios de servicio DDoS por encargo

Ataques sofisticados usan Passkeys y suplantación de CEO para comprometer cuentas de Microsoft Cloud

Microsoft ha advertido sobre campañas de phishing altamente sofisticadas que utilizan inteligencia artificial (IA), suplantación de identidad de CEO y señuelos relacionados con passkeys para defraudar a organizaciones a través de transferencias ACH y secuestrar cuentas en la nube. Estos ataques buscan eludir la autenticación multifactor (MFA) y comprometer los entornos de Microsoft Cloud, resaltando la necesidad de una vigilancia constante y una formación de seguridad robusta.

Ampliar información: Ataques sofisticados usan Passkeys y suplantacion de CEO para comprometer cuentas de Microsoft Cloud

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación de parches para las vulnerabilidades críticas con explotación activa en Cisco Identity Services Engine (plazo hasta el 19 de septiembre) y Cisco Secure Email Gateway (plazo hasta el 17 de septiembre), así como las actualizaciones para el Kernel de Linux (plazo hasta el 21 de septiembre). Monitoree su infraestructura en busca de la presencia de malware como RatHat, BambooToken y SparroWocky. Revise y fortalezca sus defensas contra ataques de phishing sofisticados y asegure sus sistemas DNS. Nuestro equipo de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está atento a los indicadores de compromiso relacionados con las amenazas de esta semana 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.