INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W41 · SEMANAL

Semana del 28 sep 2026 al 11 oct 2026 · publicado el 15 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

Edición doble que cubre las semanas 40 y 41 (28 de septiembre al 11 de octubre). CISA confirmó explotación activa de once vulnerabilidades. En la primera semana el foco estuvo en el perímetro y la colaboración: un zero-day crítico en Fortinet FortiMail (CVSS 9.8) que permite escribir archivos sin autenticación, un bypass de autenticación en Cisco Catalyst SD-WAN Manager (CVSS 9.8) que entrega privilegios de administrador, una denegación de servicio en Citrix NetScaler, una ejecución de código en Apple CoreGraphics usada en ataques dirigidos y dos fallas encadenables en Zammad. En la segunda semana el catálogo incorporó cinco fallas antiguas (ProFTPD, ONLYOFFICE Docs, Apache Struts, ISC BIND y Strapi, entre 2015 y 2023) que siguen siendo explotadas en sistemas sin mantenimiento: la antigüedad de un CVE no lo vuelve inofensivo. En amenazas, el patrón dominante es el abuso de herramientas legítimas: phishing que instala software de acceso remoto (MSP360, ScreenConnect) y la campaña CSuite que roba sesiones de Microsoft 365 a directivos; el ransomware Warlock sobre SharePoint; el backdoor Antino, que usa Outlook y OneDrive como canal de mando y control; mineros XMRig instalados mediante zero-days en AhsayCBS; y RatHat, un troyano bancario para Android que usa IA para elegir a sus víctimas. Cierra la edición el secuestro de registros DNS de tres dominios de país que permitió emitir certificados HTTPS fraudulentos para Google y YouTube, un recordatorio de que la confianza en internet también depende de la higiene del DNS. La prioridad para las próximas dos semanas: parchar el perímetro (FortiMail, SD-WAN Manager, NetScaler), forzar las actualizaciones de Apple por MDM y hacer inventario de los servicios heredados expuestos a internet.


| 11 | 11 | 5 |
|---|---|---|
| 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

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

11 vulnerabilidades, 11 con explotación activa confirmada · 5 campaña(s) de malware · 5 noticia(s) · semana del 28 sep 2026 al 11 oct 2026

## VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 10.0 | Explotación activa | CVE-2015-3306

### Lectura y escritura arbitraria de archivos en ProFTPD (mod_copy)

ProFTPD · CWE-284 · Versiones afectadas: `No especificadas por CISA; instalaciones con los comandos SITE CPFR y SITE CPTO habilitados (módulo mod_copy).`

Control de acceso insuficiente en ProFTPD que permite a un atacante remoto, sin autenticarse, leer y escribir archivos arbitrarios mediante los comandos SITE CPFR y SITE CPTO del módulo mod_copy. CISA la añadió al catálogo de explotación activa el 8 de octubre de 2026, once años después de su publicación: sigue habiendo servidores FTP expuestos sin mantenimiento.

**Impacto:** Escritura de archivos en rutas sensibles y, con ello, ejecución remota de código y toma de control total del servidor y de los datos que aloja.

> **Acción a seguir:** Actualice ProFTPD a una versión soportada o deshabilite el módulo mod_copy; si el servicio debe seguir expuesto, restrinja el acceso por origen y revise archivos creados recientemente en el sistema. Plazo de CISA: 11 de octubre de 2026 (ya vencido: trátelo como urgente).

**Ampliar información:** NVD — CVE-2015-3306 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-104286

### Zero-day en Fortinet FortiMail: escritura de archivos sin autenticación

Fortinet FortiMail · CWE-22 / CWE-158 · Versiones afectadas: `8.0.0; 7.6.0 a 7.6.5; 7.4.0 a 7.4.6; 7.2.0 a 7.2.9; 7.0.0 a 7.0.9`

Combinación de path traversal y neutralización incorrecta del carácter nulo en FortiMail que permite a un atacante no autenticado escribir archivos arbitrarios en el sistema subyacente mediante peticiones HTTP o HTTPS manipuladas. Fue explotada como zero-day antes de que existiera corrección y CISA la incorporó al catálogo el 1 de octubre de 2026.

**Impacto:** Compromiso completo de la pasarela de correo: ejecución de código, acceso al flujo de mensajes de la organización y punto de apoyo para moverse hacia el resto de la red.

> **Acción a seguir:** Actualice cada rama a la primera versión no afectada (posterior a 7.6.5, 7.4.6, 7.2.9 o 7.0.9; para 8.0.0, la corrección publicada por Fortinet). Mientras tanto, limite la exposición de la interfaz web administrativa a redes de gestión y revise archivos creados o modificados en la unidad. Plazo de CISA: 4 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-104286 CISA KEV

Crítica · CVSS 9.8 Explotación activa CVE-2026-76504

## Bypass de autenticación en Cisco Catalyst SD-WAN Manager

Cisco Catalyst SD-WAN Manager · Versiones afectadas: `17.2.10; 18.3.6; 18.3.6.1; 18.3.7; 18.3.8`

Manejo incorrecto de la codificación hexadecimal del URI en las peticiones HTTP del SD-WAN Manager. Un atacante remoto sin credenciales puede obtener acceso al sistema con los privilegios del usuario administrador. Cisco confirmó explotación activa y CISA la añadió al catálogo el 30 de septiembre de 2026.

**Impacto:** Control administrativo del plano de gestión de la red SD-WAN: cambio de políticas, redirección de tráfico y acceso a la configuración de todos los sitios conectados.

> **Acción a seguir:** Aplique la versión corregida que Cisco publica para su tren de software (17.2.10, 18.3.6, 18.3.6.1, 18.3.7 y 18.3.8 están afectadas). Hasta entonces, restrinja el acceso a la interfaz de gestión a direcciones de administración y audite las cuentas y sesiones de administrador. Plazo de CISA: 3 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-76504 CISA KEV

Crítica · CVSS 9.8 Explotación activa CVE-2021-3199

## Path traversal con ejecución remota de código en ONLYOFFICE Docs

ONLYOFFICE Docs Server · CWE-22 · Versiones afectadas: `No especificadas por CISA; instalaciones de Docs Server sin actualizar.`

Path traversal en el servidor de documentos de ONLYOFFICE que se manifiesta cuando se usa JWT: una secuencia /.. en el parámetro de carga de imágenes permite escribir fuera del directorio previsto y alcanzar ejecución remota de código. Añadida al catálogo de CISA el 8 de octubre de 2026.

**Impacto:** Ejecución de código en el servidor de edición colaborativa y acceso a los documentos que procesa, incluidos los de suites de productividad que lo integran.

> **Acción a seguir:** Actualice ONLYOFFICE Docs Server a la versión vigente del fabricante, verifique que la función de carga de imágenes no sea alcanzable sin autenticación y revise accesos recientes al servidor. Plazo de CISA: 11 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2021-3199 CISA KEV

Alta · CVSS 8.8 Explotación activa CVE-2026-86950

## Ejecución de código en CoreGraphics de iOS, iPadOS y macOS usada en ataques dirigidos

Apple iOS, iPadOS y macOS · CWE-787 · Versiones afectadas: `Anteriores a 26.7.1 y a 15.8.1`

Escritura fuera de límites en el componente CoreGraphics que puede derivar en ejecución de código arbitrario al procesar contenido gráfico manipulado. Apple publicó parches de urgencia y reconoció su uso en ataques dirigidos contra personas concretas. CISA la incorporó al catálogo el 29 de septiembre de 2026.

**Impacto:** Compromiso del dispositivo del usuario (teléfono, tableta o equipo) con acceso a su correo, mensajería y credenciales corporativas.

> **Acción a seguir:** Actualice a iOS e iPadOS 26.7.1 o 15.8.1 según la rama y a la versión equivalente de macOS; use la gestión de dispositivos móviles (MDM) para forzar la actualización en los equipos corporativos y de los directivos. Plazo de CISA: 2 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-86950 CISA KEV

Alta · CVSS 8.7 **Explotación activa** CVE-2026-102489

## Fijación de sesión con ejecución remota de código en Zammad

Zammad (mesa de ayuda) · CWE-384 · Versiones afectadas: `6.3.0 a anteriores a 6.5.4`

Fijación de sesión en la plataforma de mesa de ayuda Zammad que puede conducir a ejecución remota de código con la identidad del usuario de servicio zammad. CISA documenta que se encadena con CVE-2026-102490 para llegar a root. Añadida al catálogo el 2 de octubre de 2026.

**Impacto:** Acceso al sistema de tickets y a la información de clientes y usuarios que contiene; con el encadenamiento, control total del servidor.

> **Acción a seguir:** Actualice Zammad a 6.5.4 o posterior y revise sesiones y usuarios creados recientemente en la plataforma. Plazo de CISA: 5 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-102489 CISA KEV

Alta · CVSS 8.7 **Explotación activa** CVE-2026-88779

## Zero-day de denegación de servicio en Citrix NetScaler ADC y Gateway

Citrix NetScaler ADC y NetScaler Gateway · CWE-119 · Versiones afectadas: `Anteriores a 14.1-73.41; anteriores a 13.1-64.28; anteriores a 14.1-73.41 FIPS; anteriores a 13.1-37.282`

Restricción insuficiente de operaciones dentro de los límites de un búfer de memoria que permite provocar una denegación de servicio en NetScaler ADC y Gateway. Citrix la reportó como día cero y CISA la añadió al catálogo el 4 de octubre de 2026. Se suma a CVE-2026-88772 y CVE-2026-88771, tratadas en la edición 2026-W39; además, Citrix publicó en la segunda semana correcciones para CVE-2026-107406, que permite ejecución remota de código o denegación de servicio en configuraciones SAML y aún no figura en el catálogo de CISA.

**Impacto:** Caída del acceso remoto y de las aplicaciones publicadas a través de NetScaler; en el caso de CVE-2026-107406, posible compromiso del dispositivo.

> **Acción a seguir:** Actualice a NetScaler 14.1-73.41, 13.1-64.28 o, en builds FIPS y NDcPP, 13.1-37.282 o posteriores, y aplique en el mismo mantenimiento la corrección de CVE-2026-107406 si usa autenticación SAML. Plazo de CISA: 7 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-88779 CISA KEV

Alta · CVSS 8.5 **Explotación activa** CVE-2026-102490

## Escalada de privilegios a root en Zammad

Zammad (mesa de ayuda) · CWE-269 · Versiones afectadas: `1.5.0 a anteriores a 7.1.0-alpha`

Gestión incorrecta de privilegios que permite al usuario local zammad escalar a root. Por sí sola requiere acceso previo; encadenada con CVE-2026-102489 convierte una sesión fijada en control total del servidor. Añadida al catálogo de CISA el 2 de octubre de 2026.

**Impacto:** Control total del servidor que aloja la mesa de ayuda y de cualquier otro servicio que comparta el equipo.

> **Acción a seguir:** Actualice Zammad a la versión que corrige la escalada según el aviso del fabricante (CISA lista como afectadas las versiones anteriores a 7.1.0-alpha) y ejecute la plataforma con el mínimo privilegio necesario. Plazo de CISA: 5 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2026-102490 CISA KEV

Alta · CVSS 8.1 Explotación activa CVE-2016-3081

## Inyección de comandos en Apache Struts con invocación dinámica de métodos

Apache Struts · CWE-77 · Versiones afectadas: `No especificadas por CISA; aplicaciones Struts con la invocación dinámica de métodos (DMI) habilitada.`

Inyección de comandos en Apache Struts que permite a atacantes remotos ejecutar código arbitrario mediante el prefijo method: cuando la invocación dinámica de métodos está habilitada. Publicada en 2016 y añadida al catálogo de CISA el 8 de octubre de 2026 por explotación activa en aplicaciones heredadas.

**Impacto:** Ejecución de código en el servidor de aplicaciones Java y acceso a los datos y credenciales que maneja la aplicación.

> **Acción a seguir:** Deshabilite la invocación dinámica de métodos en la configuración de Struts y migre las aplicaciones a una versión soportada del framework; inventaríe las aplicaciones Java heredadas expuestas a internet. Plazo de CISA: 11 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2016-3081 CISA KEV

Alta · CVSS 7.5 Explotación activa CVE-2015-5477

## Denegación de servicio en ISC BIND mediante consultas TKEY

ISC BIND · CWE-19 · Versiones afectadas: `No especificadas por CISA; servidores BIND sin actualizar.`

Error de procesamiento de datos en BIND que permite a atacantes remotos provocar una denegación de servicio mediante consultas TKEY manipuladas. Es una falla de 2015 que CISA añadió al catálogo el 8 de octubre de 2026: todavía hay resolutores y servidores autoritativos expuestos que se pueden tumbar desde internet.

**Impacto:** Interrupción de la resolución DNS de la organización y, con ella, de correo, aplicaciones y acceso a internet.

> **Acción a seguir:** Actualice BIND a una versión soportada por ISC, limite las consultas recursivas a redes internas y supervise reinicios inesperados del servicio named. Plazo de CISA: 11 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2015-5477 CISA KEV

Alta · CVSS 7.2 Explotación activa CVE-2023-22894

## Exposición de información sensible en Strapi desde el panel de administración

Strapi (CMS headless) · CWE-312 · Versiones afectadas: `No especificadas por CISA; el producto afectado puede estar en fin de vida o fin de soporte.`

Almacenamiento en texto claro de información sensible en Strapi que permite a un atacante con acceso al panel de administración descubrir datos de los usuarios mediante filtros de consulta. CISA advierte que las versiones afectadas pueden estar fuera de soporte y la añadió al catálogo el 8 de octubre de 2026.

**Impacto:** Fuga de datos de usuarios y credenciales derivadas, con posibilidad de escalar hacia otras cuentas y sistemas.

> **Acción a seguir:** Actualice Strapi a una versión soportada o planifique el reemplazo de la instalación si está en fin de vida; restrinja el panel de administración a redes de confianza y active la autenticación multifactor. Plazo de CISA: 11 de octubre de 2026 (vencido).

**Ampliar información:** NVD — CVE-2023-22894 CISA KEV

## MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

### Phishing que instala software de acceso remoto legítimo (MSP360, ScreenConnect) y campaña CSuite

Microsoft advirtió sobre campañas de phishing que, en lugar de malware tradicional, llevan a la víctima a instalar herramientas de administración remota legítimas como MSP360 y ScreenConnect, con las que el atacante obtiene acceso persistente que pasa desapercibido para muchos controles. La campaña CSuite aplica el mismo patrón contra directivos: un phishing cuidado roba la sesión de Microsoft 365 y después despliega una herramienta de acceso remoto en el equipo del ejecutivo.

**MITRE ATT&CK** `T1566 — Phishing` `T1539 — Steal Web Session Cookie` `T1219 — Remote Access Software` `T1078 — Valid Accounts`

> **Acción a seguir:** Defina qué herramientas de acceso remoto están autorizadas y bloquee o alerte sobre cualquier otra con el control de aplicaciones del endpoint; exija autenticación multifactor resistente al phishing para directivos y revise en Microsoft 365 los inicios de sesión desde ubicaciones o dispositivos nuevos y las reglas de buzón creadas recientemente.

**Ampliar información:** Ataques de phishing abusan software RMM (MSP360, ScreenConnect) para acceso persistente  Campaña CSuite: phishing avanzado roba sesiones de Microsoft 365 y despliega RMM

### Ransomware Warlock (Longlegs) sobre Microsoft SharePoint

El grupo Warlock, también rastreado como Longlegs, continúa explotando vulnerabilidades de Microsoft SharePoint expuesto a internet para entrar, deshabilitar las herramientas de seguridad del servidor y desplegar ransomware. Las víctimas recientes incluyen organizaciones de infraestructura crítica en Latinoamérica y Europa.

**MITRE ATT&CK** `T1190 — Exploit Public-Facing Application` `T1562.001 — Impair Defenses: Disable or Modify Tools` `T1486 — Data Encrypted for Impact`

> **Acción a seguir:** Confirme que todos los servidores SharePoint locales tienen los parches acumulativos vigentes y no exponen la interfaz directamente a internet; proteja la configuración del antimalware contra manipulación y verifique que las copias de respaldo de SharePoint estén aisladas y probadas.

**Ampliar información:** Warlock explota vulnerabilidades de SharePoint para deshabilitar seguridad y desplegar ransomware

### Backdoor Antino: mando y control a través de Outlook y OneDrive

Antino es un backdoor compilado en Rust, atribuido a actores de espionaje vinculados a China, que usa los servicios de Microsoft 365 (Outlook y OneDrive) como canal de mando y control y de exfiltración. Al viajar sobre dominios legítimos de Microsoft, su tráfico se confunde con el uso normal de la suite.

**MITRE ATT&CK** `T1102 — Web Service` `T1567.002 — Exfiltration to Cloud Storage` `T1071.001 — Application Layer Protocol: Web Protocols`

> **Acción a seguir:** Correlacione qué procesos del endpoint se comunican con las API de Microsoft 365: un binario desconocido que habla con Outlook o OneDrive es un indicador fuerte. Revise en el tenant las aplicaciones y consentimientos OAuth concedidos recientemente y los accesos a buzones desde clientes no habituales.

**Ampliar información:** Backdoor Antino utiliza Outlook y OneDrive para C2 en campaña de espionaje vinculada a China

### Mineros XMRig instalados mediante zero-days en AhsayCBS, camuflados como Microsoft Edge

Atacantes explotan vulnerabilidades de día cero en AhsayCBS, una plataforma de respaldo, para instalar criptomineros XMRig que se hacen pasar por procesos de Microsoft Edge y así evadir la detección. Aunque el objetivo inmediato es minar criptomonedas, el acceso obtenido sobre un servidor de respaldo abre la puerta a daños mucho mayores.

MITRE ATT&CK `T1190 — Exploit Public-Facing Application` `T1036.005 — Masquerading: Match Legitimate Name or Location` `T1496 — Resource Hijacking`

> **Acción a seguir:** Retire de internet la consola de AhsayCBS y aplique las correcciones del fabricante en cuanto estén disponibles; vigile consumo anómalo de CPU en los servidores de respaldo y procesos con nombre de navegador que se ejecutan desde rutas inusuales. Un servidor de respaldo comprometido es también un riesgo para la recuperación ante ransomware.

**Ampliar información:** Atacantes explotan vulnerabilidades zero-day en AhsayCBS para desplegar mineros XMRig camuflados como Microsoft Edge

### RatHat: troyano bancario para Android que usa IA para elegir a sus víctimas

RatHat es un malware para Android que utiliza el modelo Gemini para analizar el dispositivo infectado, identificar a las víctimas de mayor valor y priorizar el robo de datos bancarios, mientras aplica técnicas de persistencia y evasión para mantenerse instalado.

MITRE ATT&CK `T1417 — Input Capture (Mobile)` `T1406 — Obfuscated Files or Information (Mobile)`

> **Acción a seguir:** Permita solo aplicaciones de las tiendas oficiales en los dispositivos corporativos mediante MDM, revise los permisos de accesibilidad concedidos a aplicaciones y refuerce con el banco la autenticación de operaciones desde dispositivos móviles.

**Ampliar información:** Malware RatHat para Android: IA Gemini prioriza víctimas y evade detección

## NOTICIAS DE CIBERSEGURIDAD lo que cambia esta semana

### Secuestro de registros DNS en tres dominios de país permitió emitir certificados HTTPS fraudulentos para Google y YouTube

Un ataque comprometió registros DNS de los dominios de país .gh, .sl y .as y, con ese control, los atacantes obtuvieron certificados HTTPS no autorizados para dominios de Google y YouTube. El incidente se detectó y mitigó, pero deja una lección para cualquier organización: el control del DNS equivale al control de la identidad en internet.

**Ampliar información:** Secuestro de registros DNS en ccTLDs permite emisión de certificados fraudulentos para dominios de Google  Secuestro de ccTLDs para emitir certificados HTTPS falsos de Google y YouTube

### Exploit público para AnyDesk en Linux: acceso root antes de autenticarse

Se publicó un exploit para una vulnerabilidad crítica de AnyDesk en Linux que permite ejecución remota de código y acceso root sin autenticación previa, por un desbordamiento de búfer. Con el exploit disponible, los equipos Linux con AnyDesk expuesto pasan a ser objetivo inmediato; la versión 8.0.3 corrige la falla.

**Ampliar información:** Exploit público de AnyDesk Linux: acceso root pre-autenticación por desbordamiento de búfer

### ShinyHunters explota CVE-2026-35273 en Oracle PeopleSoft evadiendo el WAF

El grupo ShinyHunters explota una vulnerabilidad crítica en Oracle PeopleSoft con técnicas que evaden los cortafuegos de aplicaciones web y despliega web shells para mantener el acceso. Los sistemas de nómina y recursos humanos basados en PeopleSoft concentran datos personales de alto valor, lo que explica el interés del grupo.

**Ampliar información:** Vulnerabilidad crítica en Oracle PeopleSoft con WAF bypass: ShinyHunters explota CVE-2026-35273

## CISA alerta por explotación activa en Microsoft SharePoint (CVE-2026-65660) y MikroTik RouterOS (CVE-2026-67279)

CISA exigió parches urgentes para una ejecución remota de código en Microsoft SharePoint, tratada en la edición 2026-W39, y para una falla de MikroTik RouterOS explotada en routers expuestos a internet. MikroTik es muy común en pequeñas y medianas empresas de la región, por lo que conviene revisar versión, acceso administrativo y servicios publicados en cada equipo.

**Ampliar información:** Vulnerabilidades críticas en SharePoint y MikroTik RouterOS son explotadas activamente

## Spectre-v2 BTR: nueva variante expone memoria en motores JIT de Linux, Firefox y GraalVM

Investigadores detallaron BTR, una nueva variante de Spectre-v2 que afecta a motores de compilación en tiempo de ejecución en Linux, Firefox y GraalVM, permite filtrar datos sensibles de la memoria y elude las mitigaciones existentes. Ya hay parches disponibles; el riesgo práctico es mayor en servidores multiusuario y en entornos que ejecutan código de terceros.

**Ampliar información:** Nueva variante Spectre-v2 BTR expone memoria Linux y elude defensas existentes

ACCIÓN A SEGUIR

## Cómo te acompaña nuestro SOC

Acciones prioritarias para las próximas dos semanas: 1) **Perímetro y correo (plazos de CISA ya vencidos, trátelos como emergencia):** actualice Fortinet FortiMail (CVE-2026-104286), Cisco Catalyst SD-WAN Manager (CVE-2026-76504) y Citrix NetScaler ADC/Gateway (CVE-2026-88779, junto con CVE-2026-107406 si usa SAML). Si no puede parchar hoy, restrinja las interfaces administrativas a redes de gestión y busque indicios de compromiso: archivos nuevos en FortiMail, cuentas o sesiones de administrador inesperadas en SD-WAN Manager. 2) **Dispositivos y colaboración:** fuerce por MDM la actualización de iPhone, iPad y Mac a 26.7.1 o 15.8.1 (CVE-2026-86950) y lleve Zammad a 6.5.4 o posterior (CVE-2026-102489 y CVE-2026-102490). 3) **Servicios heredados expuestos:** inventaríe ProFTPD, ISC BIND, Apache Struts, ONLYOFFICE Docs y Strapi alcanzables desde internet; actualícelos o retírelos. Que los CVE tengan entre tres y once años demuestra que los atacantes siguen encontrándolos. 4) **Vigilancia de esta edición:** instalaciones no autorizadas de herramientas de acceso remoto (MSP360, ScreenConnect, AnyDesk) y sesiones de Microsoft 365 anómalas en cuentas directivas (CSuite); procesos desconocidos que se comunican con Outlook o OneDrive (Antino); servidores SharePoint locales expuestos (Warlock); consumo anómalo de CPU en servidores de respaldo (XMRig en AhsayCBS); routers MikroTik con administración publicada. 5) **DNS e identidad digital:** publique registros CAA para sus dominios, habilite DNSSEC donde el registrador lo permita y supervise los registros de transparencia de certificados. Nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) incorpora estos indicadores en la vigilancia continua de los clientes.

**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.