INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W29 · SEMANAL

Semana del 13 jul 2026 al 19 jul 2026 · publicado el 20 de julio 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

El boletín de esta semana destaca una serie de vulnerabilidades críticas bajo explotación activa que exigen atención inmediata. Productos como Microsoft SharePoint, Oracle E-Business Suite y Fortinet FortiSandbox presentan fallas de alta severidad que pueden conducir a la ejecución remota de código o toma de control. Adicionalmente, se observan sofisticadas campañas de phishing que eluden la MFA y el malware OkoBot, que apunta al robo de frases de recuperación de wallets de criptomonedas. Es imperativo que las organizaciones prioricen la aplicación de parches y refuercen sus defensas contra las amenazas emergentes.

8	8	2
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

5	2	1	0
CRÍTICA	ALTA	MEDIA	BAJA
CVSS 9,0 – 10	CVSS 7,0 – 8,9	CVSS 4,0 – 6,9	CVSS 0,1 – 3,9

8 vulnerabilidades, 8 con explotación activa confirmada · 2 campaña(s) de malware · 4 noticia(s) · semana del 13 jul 2026 al 19 jul 2026

VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 10.0 | Explotación activa | CVE-2026-15409

Vulnerabilidad de Falsificación de Solicitudes en el Servidor (SSRF) en SonicWall SMA1000 Appliances

SonicWall SMA1000 Appliances · Versiones afectadas: `12.4.3-03245 – ≤12.4.3-03434; 12.5.0-02283 – ≤12.5.0-02800`

SonicWall SMA1000 Appliances contiene una vulnerabilidad de falsificación de solicitudes en el servidor (SSRF) que podría permitir que un atacante remoto no autenticado fuerce al dispositivo a realizar solicitudes a ubicaciones no intencionadas.

Impacto: La explotación exitosa puede permitir a un atacante no autenticado interactuar con servicios internos, acceder a información sensible o ejecutar acciones no autorizadas, comprometiendo la confidencialidad y la integridad del sistema.

> **Acción a seguir:** Actualizar los dispositivos SonicWall SMA1000 a versiones parcheadas que superen la 12.4.3-03434 y la 12.5.0-02800. Plazo de CISA: 17 de julio de 2026.

Ampliar información: NVD — CVE-2026-15409 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-58644

Vulnerabilidad de Deserialización de Datos no Confiables en Microsoft SharePoint

Microsoft SharePoint · Versiones afectadas: `16.0.0 – <16.0.5556.1005; 16.0.0 – <16.0.10417.20153; 16.0.0 – <16.0.19725.20384`

Microsoft SharePoint contiene una vulnerabilidad de deserialización de datos no confiables que permite a un atacante no autorizado ejecutar código a través de la red.

Impacto: Esta falla crítica posibilita la ejecución remota de código (RCE) por parte de un atacante no autenticado, lo que puede resultar en el control total del servidor SharePoint afectado.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft para SharePoint que aborden las versiones 16.0.5556.1005, 16.0.10417.20153 y 16.0.19725.20384. Plazo de CISA: 19 de julio de 2026.

Ampliar información: NVD — CVE-2026-58644 CISA KEV

Crítica · CVSS 9.8 | Explotación activa | CVE-2026-46817

Vulnerabilidad de Gestión de Privilegios Inapropiada en Oracle E-Business Suite

Oracle E-Business Suite · Versiones afectadas: `12.2.3 – ≤12.2.15`

Oracle E-Business Suite contiene una vulnerabilidad de gestión de privilegios inapropiada que permite a un atacante no autenticado con acceso a la red a través de HTTP comprometer Oracle Payments.

Impacto: Un atacante puede tomar el control de Oracle Payments, lo que conlleva graves riesgos financieros, de confidencialidad de datos y de integridad de transacciones.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Oracle que aborden las versiones 12.2.15 y anteriores para E-Business Suite. Plazo de CISA: 18 de julio de 2026.

Ampliar información: NVD — CVE-2026-46817 CISA KEV

Crítica · CVSS 9.1 Explotación activa CVE-2026-39808

Vulnerabilidad de Inyección de Comandos del Sistema Operativo en Fortinet FortiSandbox

Fortinet FortiSandbox · Versiones afectadas: `4.4.0 – ≤4.4.8; 23.4.4374; 23.4.4350; 23.3.4329; 23.1.4245`

Fortinet FortiSandbox contiene una vulnerabilidad de inyección de comandos del sistema operativo que podría permitir a un atacante no autenticado ejecutar código o comandos no autorizados mediante solicitudes HTTP manipuladas.

Impacto: La explotación resulta en la ejecución remota de código por parte de un atacante no autenticado, lo que puede llevar a la toma de control del sistema y la exfiltración de datos.

> **Acción a seguir:** Actualizar Fortinet FortiSandbox a versiones posteriores a las afectadas: 4.4.8, 23.4.4374, 23.4.4350, 23.3.4329 y 23.1.4245. Plazo de CISA: 19 de julio de 2026.

Ampliar información: NVD — CVE-2026-39808 CISA KEV

Crítica · CVSS 9.1 Explotación activa CVE-2026-25089

Vulnerabilidad de Inyección de Comandos del Sistema Operativo en Fortinet FortiSandbox, Cloud y PaaS

Fortinet FortiSandbox · Versiones afectadas: `5.0.0 – ≤5.0.5; 4.4.0 – ≤4.4.8; 4.2.1 – ≤4.2.8; 5.0.4 – ≤5.0.5`

Fortinet FortiSandbox, FortiSandbox Cloud y FortiSandbox PaaS contienen una vulnerabilidad de inyección de comandos del sistema operativo que permite a un atacante no autenticado ejecutar comandos no autorizados mediante solicitudes HTTP específicamente manipuladas.

Impacto: Permite la ejecución remota de comandos por parte de un atacante no autenticado, resultando en la toma de control total del sistema y acceso a los recursos gestionados.

> **Acción a seguir:** Actualizar Fortinet FortiSandbox, FortiSandbox Cloud y FortiSandbox PaaS a versiones que superen la 5.0.5, 4.4.8 y 4.2.8. Plazo de CISA: 19 de julio de 2026.

Ampliar información: NVD — CVE-2026-25089 CISA KEV

Alta · CVSS 7.8 Explotación activa CVE-2026-56155

Vulnerabilidad de Granularidad Insuficiente de Control de Acceso en Microsoft Active Directory Federation Services

Microsoft Active Directory Federation Services · Versiones afectadas: `10.0.14393.0 – <10.0.14393.9339; 10.0.17763.0 – <10.0.17763.9020; 6.2.9200.0 – <6.2.9200.26226; 6.3.9600.0 – <6.3.960…`

Microsoft Active Directory Federation Services (ADFS) contiene una vulnerabilidad de granularidad insuficiente de control de acceso que permite a un atacante autorizado elevar privilegios localmente.

Impacto: Un atacante con privilegios bajos puede escalar sus privilegios dentro del sistema, obteniendo acceso no autorizado a recursos y datos sensibles.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft ADFS que aborden las versiones 10.0.14393.9339, 10.0.17763.9020, 6.2.9200.26226 y la serie 6.3.9600.x. Plazo de CISA: 28 de julio de 2026.

Ampliar información: NVD — CVE-2026-56155 CISA KEV

Alta · CVSS 7.2 **Explotación activa** CVE-2026-15410

Vulnerabilidad de Inyección de Código en SonicWall SMA1000 Appliances

SonicWall SMA1000 Appliances · Versiones afectadas: `12.4.3-03245 – ≤12.4.3-03434; 12.5.0-02283 – ≤12.5.0-02800`

SonicWall SMA1000 Appliances contiene una vulnerabilidad de inyección de código que, bajo condiciones específicas, podría permitir a un atacante remoto autenticado como administrador ejecutar comandos arbitrarios del sistema operativo.

Impacto: La explotación permite la ejecución de comandos arbitrarios por parte de un administrador autenticado, comprometiendo potencialmente el dispositivo y su entorno de red.

> **Acción a seguir:** Actualizar los dispositivos SonicWall SMA1000 a versiones parcheadas que superen la 12.4.3-03434 y la 12.5.0-02800. Plazo de CISA: 17 de julio de 2026.

Ampliar información: NVD — CVE-2026-15410 CISA KEV

Media · CVSS 5.3 **Explotación activa** CVE-2026-56164

Vulnerabilidad de Autenticación Faltante para Función Crítica en Microsoft SharePoint Server

Microsoft SharePoint Server · Versiones afectadas: `16.0.0 – <16.0.5561.1001; 16.0.0 – <16.0.10417.20175; 16.0.0 – <16.0.19725.20434`

Microsoft SharePoint contiene una vulnerabilidad de autenticación faltante para una función crítica que permite a un atacante no autorizado elevar privilegios a través de la red.

Impacto: Un atacante no autenticado puede elevar sus privilegios, obteniendo acceso a recursos o funcionalidades que de otro modo estarían restringidas, comprometiendo la seguridad del servidor.

> **Acción a seguir:** Aplicar las actualizaciones de seguridad de Microsoft para SharePoint Server que superen las versiones 16.0.5561.1001, 16.0.10417.20175 y 16.0.19725.20434. Plazo de CISA: 17 de julio de 2026.

Ampliar información: NVD — CVE-2026-56164 CISA KEV

MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

OkoBot

OkoBot es un framework de malware diseñado para inyectar código de phishing en aplicaciones legítimas de wallets de criptomonedas como Ledger y Trezor. Su objetivo principal es robar las frases de recuperación (frases semilla) de los usuarios, comprometiendo activos digitales en más de 25 países.

MITRE ATT&CK `T1566 — Phishing` `T1055 — Process Injection` `T1552.001 — Credentials in Files`

> **Acción a seguir:** Para proteger sus activos digitales, implemente autenticación multifactor (MFA) robusta en los exchanges, utilice wallets de hardware y verifique siempre las URL y mensajes antes de ingresar credenciales o frases de recuperación. Mantenga el sistema operativo y las aplicaciones de seguridad actualizados para detectar y prevenir la inyección de código malicioso.

Ampliar información: OkoBot: Malware Inyecta Phishing para Robar Frases de Recuperación de Wallets Cripto

Campañas de Phishing con Evilginx

Se han detectado campañas de phishing sofisticadas que utilizan el framework Evilginx y abusan del flujo de código de dispositivo para evadir la autenticación multifactor (MFA) en entornos de Microsoft 365. Los atacantes explotan la confianza inherente en los dispositivos y servicios para eludir las barreras de seguridad tradicionales y obtener acceso a cuentas corporativas, representando una amenaza significativa para la identidad y el acceso.

MITRE ATT&CK `T1566 — Phishing` `T1078.004 — Cloud Accounts` `T1550.002 — Steal Application Access Token`

> **Acción a seguir:** Reforzar las políticas de Acceso Condicional en Microsoft 365 para restringir el acceso desde ubicaciones o dispositivos no confiables. Capacitar a los usuarios para identificar intentos de phishing sofisticados que manipulan flujos de autenticación. Monitorear logs de autenticación para detectar patrones de acceso inusuales y posibles abusos del flujo de código de dispositivo.

Ampliar información: Ataques de phishing con Evilginx e IPs comprometidas evaden MFA en Microsoft 365

NOTICIAS DE CIBERSEGURIDAD lo que cambia esta semana

EE. UU. Sanciona Facilitadores de Ransomware y Alerta sobre Explotación Rusa de Routers en Infraestructuras Críticas

El Tesoro de EE. UU. ha impuesto sanciones a servicios VPN y vendedores de 'cryptors' por facilitar operaciones de ransomware a nivel global. Paralelamente, se ha emitido una alerta sobre ataques rusos dirigidos a routers de infraestructuras críticas, explotando vulnerabilidades conocidas (CVEs) para obtener acceso y control. Estas acciones subrayan la creciente presión sobre los ciberdelincuentes y la necesidad de proteger el perímetro de las redes críticas contra actores patrocinados por estados.

Ampliar información: Sanciones a VPNs y cryptores de ransomware; Rusia explota routers en infraestructuras críticas EE. UU. sanciona VPN y vendedor de cryptors por apoyar ransomware; alerta sobre routers explotados por Rusia

Microsoft Corrige un Número Récord de Vulnerabilidades, Incluyendo Dos Zero-Days Bajo Ataque Activo

El Patch Tuesday de julio de 2026 de Microsoft ha sido notable por corregir un número récord de 622 vulnerabilidades. Destacan dos zero-days críticos, CVE-2026-58644 en SharePoint Server y CVE-2026-56155 en Active Directory Federation Services, ambos ya bajo explotación activa. Estas actualizaciones son cruciales para mitigar riesgos significativos en entornos empresariales y deben aplicarse con prioridad para proteger los sistemas.

Ampliar información: Alerta: Microsoft corrige 622 vulnerabilidades récord, incluyendo 2 Zero-Days bajo ataque activo

Revelado Zero-Day "LegacyHive" de Elevación de Privilegios en Windows Post-Patch Tuesday

Un investigador ha revelado una nueva vulnerabilidad zero-day, denominada "LegacyHive", en Windows. Esta falla de elevación de privilegios persiste sin un parche oficial tras el Patch Tuesday reciente, lo que representa un riesgo para los sistemas Windows que aún no tienen una mitigación oficial. Las organizaciones deben estar atentas a futuras actualizaciones y recomendaciones de seguridad de Microsoft.

Ampliar información: Zero-Day en Windows Revelado Post-Patch Tuesday: Vulnerabilidad de Elevación de Privilegios

Actualizaciones Críticas para Firefox, Chrome, Adobe y VMware

Se han liberado parches de seguridad críticos para navegadores web populares como Firefox y Chrome, así como para aplicaciones empresariales clave de Adobe (ColdFusion, Commerce) y VMware Avi Load Balancer. Estas actualizaciones abordan riesgos significativos como la ejecución remota de código y la escalada de privilegios, siendo imperativa su aplicación inmediata para proteger los sistemas contra diversas amenazas.

Ampliar información: Vulnerabilidades críticas en Firefox, Chrome, Adobe y VMware exigen actualización inmediata

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

1. **Priorizar Parches Críticos (Plazo 17 de julio de 2026):** Actualizar SonicWall SMA1000 Appliance (CVE-2026-15409, CVE-2026-15410) y Microsoft SharePoint Server (CVE-2026-56164) para mitigar riesgos de ejecución de código y elevación de privilegios en sistemas expuestos. 2. **Aplicar Parches de Alta Prioridad (Plazo 18-19 de julio de 2026):** Actualizar Oracle E-Business Suite (CVE-2026-46817), Microsoft SharePoint (CVE-2026-58644) y Fortinet FortiSandbox (CVE-2026-39808, CVE-2026-25089) debido a su criticidad y explotación activa. 3. **Fortalecer Defensas Anti-Phishing:** Implementar políticas de Acceso Condicional para Microsoft 365, restringiendo el acceso desde IPs o dispositivos no autorizados, y capacitar a los usuarios sobre las tácticas de phishing con Evilginx y OkoBot para la protección de wallets de criptomonedas. 4. **Revisar Configuración de Routers:** Asegurarse de que los routers en infraestructuras críticas estén actualizados y endurecidos contra posibles explotaciones, en respuesta a las alertas de ataques patrocinados por estados. 5. **Actualizaciones Generales:** Aplicar diligentemente los parches de Microsoft Patch Tuesday y las actualizaciones críticas para navegadores (Firefox, Chrome), Adobe y VMware. Nuestro equipo está listo para ayudar con el monitoreo y respuesta gestionada (FortiGuard SOCaaS) 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.