GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3525

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	4	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	1	0	0

VULNERABILIDADES

VULNERABILIDAD 0-DAY EN APPLE IMAGEIO (CVE-2025-43300) EXPLOTADA EN ATAQUES DIRIGIDOS

El 20 de agosto de 2025, Apple liberó actualizaciones de seguridad para iOS, iPadOS y macOS, corrigiendo una vulnerabilidad crítica de escritura fuera de límites en ImageIO. La falla, identificada como CVE-2025-43300 (CVSS 8.8), está siendo explotada activamente en ataques dirigidos considerados de alta sofisticación, probablemente vinculados a espionaje y uso de spyware avanzado.

Recursos afectados:

- iOS 18.6.2: iPhone XS y posteriores.
- iPadOS 18.6.2 / 17.7.10: iPad Pro (13", 12.9", 11"), iPad Air 3ª gen y posteriores, iPad 7ª gen y posteriores, iPad mini 5ª gen y posteriores.

- macOS: Sequoia 15.6.1, Sonoma 14.7.8, Ventura 13.7.8.

Resumen técnico:

- **CVE-2025-43300 – Escritura fuera de límites en ImageIO.**
- Impacto: Procesar una imagen maliciosa puede producir corrupción de memoria y ejecución de código arbitrario.
- Descubrimiento: Reportado internamente por Apple.
- Explotación: Confirmada en ataques "extremadamente sofisticados" contra individuos específicos.
- Corrección: Mejoras en la verificación de límites (improved bounds checking).

Impacto potencial:

- Ejecución remota de código en dispositivos Apple ampliamente desplegados en entornos corporativos.
- Uso en ataques de espionaje, con alto riesgo de despliegue de spyware contra objetivos de alto perfil.
- Posible cadena con otras vulnerabilidades previamente explotadas en Safari y WebKit.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a las últimas versiones de iOS, iPadOS y macOS.
2. Habilitar actualización forzada en dispositivos corporativos y de teletrabajo.
3. Monitorear indicadores de compromiso en dispositivos Apple que hayan estado expuestos a archivos o imágenes sospechosas.

Prioridad: Crítica.

Ampliar Información:

- https://support.apple.com/en-us/124925

- https://thehackernews.com/2025/08/apple-patches-cve-2025-43300-zero-day.html
- https://www.darkreading.com/vulnerabilities-threats/apple-zero-day-flaw-sophisticated-attack
- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidad-0-day-explotada-en-varios-productos-de-apple-en-ataques-dirigidos/webcyb00-contcibglos/es/

VULNERABILIDAD CRÍTICA EN DOCKER DESKTOP PARA WINDOWS Y MACOS (CVE-2025-9074)

El 25 de agosto de 2025, investigadores revelaron una vulnerabilidad crítica en Docker Desktop para Windows y macOS que permite a un contenedor malicioso comprometer el host y escapar de su confinamiento, incluso con la función de Aislamiento Mejorado de Contenedores (ECI) habilitada.

Docker confirmó el problema y publicó parches en la versión v4.44.3, calificando la falla como crítica (CVSS 9.3).

Resumen técnico:

- **CVE-2025-9074 (SSRF, CVSS 9.3):** un contenedor puede acceder sin autenticación a la API de Docker Engine en 192.168.65.7:2375.
- Permite crear y lanzar contenedores adicionales mediante simples solicitudes HTTP (/containers/create y /containers/{id}/start), sin necesidad de montar el socket de Docker.
- PoC disponible: tres líneas de Python bastan para explotar la vulnerabilidad y montar el disco C:\ del host en un contenedor.
- Vector alternativo: explotación vía SSRF como canal para interactuar con la API interna.

Impacto por plataforma:

Windows (WSL2): acceso como administrador al sistema host, lectura de cualquier archivo y posibilidad de sobrescribir DLLs para escalar privilegios.

macOS: menor riesgo, ya que montar directorios requiere confirmación del usuario; sin embargo, el atacante puede alterar la configuración de Docker Desktop o insertar backdoors.

Linux: no afectado, al usar un pipe en lugar de socket TCP.

Impacto potencial:

- Compromiso total de hosts Windows en entornos de desarrollo.
- Robo y modificación de archivos sensibles en entornos corporativos.
- Riesgo de persistencia mediante backdoors en instalaciones de macOS.
- Posible uso en cadenas de ataque de supply chain con contenedores maliciosos.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a Docker Desktop v4.44.3 o posterior.
2. Deshabilitar ejecución de contenedores no confiables.
3. Monitorear conexiones internas hacia la API 192.168.65.7:2375.
4. Aplicar segmentación estricta y políticas de privilegios mínimos en entornos de virtualización.

Prioridad: Crítico

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/vulnerabilidad-critica-en-docker.html

- https://thehackernews.com/2025/08/docker-fixes-cve-2025-9074-critical.html
- https://docs.docker.com/desktop/release-notes/#4443

CITRIX NETSCALER – CVE-2025-7775 (EXPLOTACIÓN ACTIVA)

El 27 de agosto de 2025, la CISA (U.S. Cybersecurity and Infrastructure Security Agency) agregó la vulnerabilidad CVE-2025-7775 en Citrix NetScaler ADC y NetScaler Gateway a su catálogo de Known Exploited Vulnerabilities (KEV), confirmando explotación activa en entornos no parcheados.

Resumen técnico:

- **CVE-2025-7775 (CVSS 9.2):** Desbordamiento de memoria que permite ejecución remota de código (RCE) o denegación de servicio (DoS).
  Afecta instancias configuradas como Gateway (VPN, ICA Proxy, CVPN, RDP Proxy) o servidores virtuales HTTP/SSL/QUIC con IPv6.
- **CVE-2025-7776 (CVSS 8.8):** Otro desbordamiento de memoria que causa DoS en configuraciones con perfil PCoIP.
- **CVE-2025-8424 (CVSS 8.7):** Control de acceso indebido en la interfaz de administración de NetScaler.
- No existen soluciones alternativas (workarounds).
- Más de 28.000 instancias expuestas en internet, según reportes de seguridad independientes.

Impacto potencial:

- Compromiso total de appliances Citrix en uso como VPN empresarial.
- Posible movimiento lateral hacia redes internas de agencias y empresas.
- Riesgo crítico para infraestructuras gubernamentales, financieras y de salud.

Recomendaciones de mitigación:

1. Aplicar inmediatamente las versiones seguras: 14.1-47.48+, 13.1-59.22+, 13.1-FIPS/NDcPP 13.1-37.241+, 12.1-FIPS/NDcPP 12.1-55.330+.
2. Limitar exposición de NetScaler a internet y restringir acceso a la interfaz de administración (NSIP, SNIP, Cluster IP).
3. Revisar registros de explotación y actividad sospechosa en appliances no parcheados.
4. Seguir el Binding Operational Directive (BOD) 22-01 que obliga a agencias federales de EE.UU. a parchear antes del 28 de agosto de 2025.

Prioridad: Crítica.

Ampliar Información:

- https://securityaffairs.com/181615/security/u-s-cisa-adds-citrix-netscaler-flaw-to-its-known-exploited-vulnerabilities-catalog-2.htm
- https://thehackernews.com/2025/08/citrix-patches-three-netscaler-flaws.html
- https://www.scworld.com/news/citrix-patches-critical-zero-day-two-other-flaws
- https://www.bleepingcomputer.com/news/security/over-28-200-citrix-instances-vulnerable-to-actively-exploited-rce-bug/

VULNERABILIDAD CRÍTICA EN CISCO IOS/IOS XE – SMART INSTALL (CVE-2018-0171)

El PSIRT de Cisco publicó una actualización el 20 de agosto de 2025 confirmando que la vulnerabilidad crítica en la función Smart Install de Cisco IOS e IOS XE (CVE-2018-0171, CVSS 9.8) sigue siendo explotada activamente en campañas recientes.

Resumen técnico:

- **CVE-2018-0171 (CWE-787): Validación inadecuada de datos en Smart Install (TCP/4786) que permite a un atacante remoto no autenticado:**

Ejecutar código arbitrario en el dispositivo.
Provocar denegación de servicio (DoS) reiniciando el equipo.
Forzar bucles indefinidos que terminan en watchdog crash.

- Afecta a switches con Smart Install habilitado por defecto en versiones antiguas.
- No existen workarounds oficiales salvo deshabilitar Smart Install con no vstack.

Impacto potencial:

- Ejecución remota de código con privilegios completos en routers/switches.
- Compromiso total de infraestructuras de red corporativas y críticas.
- Alta probabilidad de explotación activa debido a actividad confirmada en campo.

Recomendaciones de mitigación:

5. Actualizar inmediatamente a las versiones corregidas de IOS/IOS XE publicadas por Cisco.
6. Deshabilitar Smart Install en dispositivos donde no sea requerido.
7. Monitorear tráfico hacia TCP/4786 e implementar reglas Snort 46096, 46097 y 46468.
8. Verificar exposición pública de equipos y segmentar accesos de administración.

Prioridad: Crítica.

Ampliar Información:

- https://csirt.axtel.com.mx/bulletin/post/355
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
- https://thehackernews.com/2025/08/fbi-warns-russian-fsb-linked-hackers.html
- https://www.securityweek.com/russian-apt-exploiting-7-year-old-cisco-vulnerability-fbi/

Recomendaciones Generales Sobre Vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Server
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

VSHELL DISTRIBUIDO MEDIANTE ARCHIVOS RAR MALICIOSOS

Investigadores de Trellix descubrieron el 23 de agosto de 2025 una campaña de phishing que distribuye el backdoor VShell en sistemas Linux mediante un vector inusual: nombres de archivo maliciosos dentro de archivos RAR. El payload no reside en el contenido del archivo, sino en el nombre del archivo, que incluye comandos de Bash codificados en Base64 capaces de ejecutarse automáticamente si son interpretados por scripts vulnerables.

Resumen técnico:

- Inicio del ataque: correo electrónico de phishing con archivo adjunto yy.rar.
- El archivo contiene nombres maliciosos como: ziliao2.pdf`{echo,}|{base64,-d}|bash`
- El shell interpreta el nombre y ejecuta un descargador codificado en Base64.

- El descargador obtiene un binario ELF adaptado a la arquitectura del sistema.
- El ELF establece conexión con un servidor remoto y despliega el backdoor VShell.
- VShell es una herramienta de acceso remoto en Go, usada por grupos como UNC5174, que permite: shell inverso, gestión de archivos/procesos, reenvío de puertos y comunicaciones C2 cifradas.
- El ataque explota la falta de validación en scripts de shell y evade antivirus, ya que estos no analizan nombres de archivo.

Impacto potencial:

- Ejecución remota de código en sistemas Linux.
- Acceso persistente y control total del host mediante VShell.
- Riesgo elevado para entornos corporativos que procesen archivos comprimidos sin validación adecuada.

Recomendaciones de mitigación:

1. Bloquear y filtrar correos de phishing con adjuntos RAR sospechosos.
2. Evitar el uso de eval o llamadas inseguras en scripts de shell.
3. Implementar análisis de nombres de archivo en motores de seguridad.
4. Monitorizar conexiones C2 relacionadas con VShell y descargas ELF inusuales.

Prioridad: Urgente

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/malware-de-linux-distribuido-traves-de.html
- https://thehackernews.com/2025/08/linux-malware-delivered-via-malicious.html
- https://www.cert.gov.py/nueva-cadena-de-infeccion-de-malware-linux-vshell-ringreaper/

- https://enhacke.com/blog/rar-malicioso-instala-malware-en-linux-68a884f745692

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

FBI ALERTA SOBRE EXPLOTACIÓN DE CVE-2018-0171 POR GRUPO RUSO

El PSIRT de Cisco y el FBI confirmaron el 20 de agosto de 2025 que la vulnerabilidad crítica en la función Smart Install de Cisco IOS e IOS XE (CVE-2018-0171, CVSS 9.8) sigue siendo explotada activamente en campañas de ciberespionaje atribuidas al grupo ruso Static Tundra (FSB – Centro 16).

Resumen técnico:

- CVE-2018-0171 (CWE-787): Validación inadecuada de datos en Smart Install (TCP/4786).
- Permite a un atacante remoto no autenticado:
  - Ejecutar código arbitrario en el dispositivo.
  - Provocar denegación de servicio (DoS) con reinicio forzado.
  - Inducir bucles indefinidos que finalizan en watchdog crash.
- Afecta a routers y switches con Smart Install habilitado por defecto en versiones antiguas.
- Explotación activa confirmada:
  - Implantación de SYNful Knock para persistencia.
  - Uso de SNMP para alterar configuraciones y evadir registros.
  - Creación de túneles GRE para desviar tráfico sensible.
  - Exfiltración de configuraciones y datos NetFlow vía TFTP/FTP.
- Históricamente también explotada por grupos chinos (Salt Typhoon) en 2024.

Impacto potencial:

- Compromiso total de infraestructuras críticas y corporativas mediante ejecución remota de código con privilegios de administrador.
- Persistencia y espionaje estratégico en sectores de telecomunicaciones, educación superior, manufactura y entidades críticas en EE.UU., Europa, Asia y África.
- Riesgo elevado de exfiltración de información sensible y movimiento lateral en entornos corporativos.

Recomendaciones para mitigar el riesgo:

- Actualizar inmediatamente a las versiones corregidas de Cisco IOS/IOS XE (14.1-47.48+, 13.1-59.22+, 13.1-FIPS/NDcPP 13.1-37.241+, 12.1-FIPS/NDcPP 12.1-55.330+).

- Deshabilitar Smart Install en dispositivos donde no sea requerido (no vstack).
- Monitorear tráfico anómalo en TCP/4786 e implementar reglas Snort 46096, 46097 y 46468.
- Auditar accesos a configuraciones de red y revisar indicadores de manipulación en SNMP/TACACS+.
- Limitar la exposición pública de equipos y segmentar accesos de administración.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/08/fbi-warns-russian-fsb-linked-hackers.html
- https://www.securityweek.com/russian-apt-exploiting-7-year-old-cisco-vulnerability-fbi/
- https://devel.group/blog/la-ofensiva-rusa-contra-la-infraestructura-digital-global/
- https://industrialcyber.co/threats-attacks/russian-fsb-center-16-exploits-decade-old-cisco-flaw-in-cyber-espionage-campaign-to-target-critical-infrastructure/