GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4025

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	3	0	0
MALWARE	0	0	1
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

CVE-2025-41244 — VMWARE TOOLS Y ARIA (ZERO-DAY PRIVILEGE ESCALATION)

Un zero-day de escalada de privilegios local en VMware Tools y VMware Aria Operations (CVSS 7.8) está siendo explotado en la naturaleza. El fallo es una debilidad de Untrusted Search Path (CWE-426) en el script get-versions.sh usado por el mecanismo de service discovery. Un actor local no privilegiado puede colocar un ejecutable malicioso en un directorio con permisos de escritura (por ejemplo /tmp/httpd). Cuando el proceso de descubrimiento ejecuta ese binario para obtener su versión, lo hace con los privilegios del servicio de VMware, lo que puede derivar en ejecución de código como root.

Resumen técnico:

- La vulnerabilidad se manifiesta en dos vectores:
- *Credential-less service discovery en VMware Tools, desplegado en VMs huésped.*
- *Legacy credential-based discovery en Aria Operations.*

- Confirmado también en la versión open-source (open-vm-tools) presente en la mayoría de distribuciones Linux.
- Explotación activa atribuida al grupo UNC5174, con reportes de incidentes desde mediados de 2024.

Impacto potencial:

- Escalada local de privilegios hasta root en entornos virtualizados.
- Compromiso de VMs huésped con control total sobre el sistema.
- Riesgo de uso en campañas de espionaje o intrusión, facilitando persistencia y movimientos laterales.
- Potencial abuso de técnicas comunes de nombrado de binarios maliciosos que se camuflan como procesos legítimos (ej. httpd).

Recomendaciones de mitigación:

1. Aplicar de inmediato los parches de Broadcom/VMware: Aria Operations → versión 8.18.5, VMware Tools → 13.0.5 y 12.5.4 y Cloud Foundation → 9.0.1.0 o parche KB92148.
2. Restringir permisos de escritura en directorios temporales (/tmp, /var/tmp), idealmente con opciones noexec y nodev.
3. Monitorizar procesos hijos inusuales de vmtoolsd o get-versions.sh, así como la creación de archivos en /tmp/VMware-SDMP-Scripts-{UUID}/.
4. Limitar la conectividad de VMs a redes internas y segmentar entornos críticos.
5. Realizar hunting para detectar posibles compromisos históricos en logs y sistemas afectados.

Prioridad: Crítica.

Ampliar Información:

- https://cybersecuritynews.com/vmware-tools-0-day-vulnerability/
- https://socprime.com/es/blog/cve-2025-41244-zero-day-vulnerability/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidades-criticas-en-vmware-aria-operations-y-vmware-tools/

CVE-2025-20333 Y CVE-2025-20362 — CISCO ASA/FTD (ZERO-DAY BAJO EXPLOTACIÓN ACTIVA)

Cisco ha confirmado la explotación activa de dos vulnerabilidades críticas en Cisco Secure Firewall Adaptive Security Appliance (ASA) y Firewall Threat Defense (FTD). Estas fallas están siendo aprovechadas en una campaña global atribuida al grupo UAT4356 (Storm-1849), vinculado con la operación ArcaneDoor.

Resumen técnico:

- CVE-2025-20333 (CVSS 9.9, Crítica): validación incorrecta de entradas en el servidor web VPN. Un atacante remoto con credenciales VPN válidas puede enviar peticiones HTTP manipuladas para lograr ejecución de código arbitrario como root en el dispositivo afectado.
- CVE-2025-20362 (CVSS 6.5, Media): validación deficiente en solicitudes HTTP(S) que permite a un atacante remoto no autenticado acceder a URLs restringidas sin credenciales.
- Explotación en curso afecta a múltiples ramas de ASA (9.16–9.22) y FTD (7.0–7.6).
- Se han detectado ataques que encadenan ambas vulnerabilidades para evadir autenticación y ejecutar código con privilegios de administrador.

- CISA emitió la Directiva de Emergencia ED 25-03, obligando a agencias federales a aplicar mitigaciones en menos de 24h.
- Los atacantes también habrían manipulado la ROM de ASA para mantener persistencia tras reinicios o actualizaciones.

Impacto potencial:

- Compromiso total de firewalls ASA/FTD, habilitando control remoto y persistencia a nivel de firmware.
- Riesgo elevado de exfiltración de credenciales, espionaje de tráfico VPN y acceso a redes internas.
- Potencial uso de malware asociado a ArcaneDoor, como Line Runner y Line Dancer, para post-explotación.
- Amenaza crítica para infraestructuras de perímetro en gobiernos, operadores críticos y grandes empresas.

Recomendaciones de mitigación:

1. Aplicar inmediatamente los parches de Cisco: ASA → versiones 9.16.4.85, 9.17.1.45, 9.18.4.47, 9.19.1.37, 9.20.3.7, 9.22.1.3 y FTD → versiones 7.0.8.1, 7.2.9, 7.4.2.4, 7.6.1.
2. Inventariar todos los dispositivos ASA/FTD expuestos y validar su versión con la herramienta *Cisco Software Checker*.
3. Realizar análisis forense de memoria (core dumps) siguiendo la guía de CISA para identificar posibles implantes en la ROM.
4. Desconectar y reemplazar equipos End of Support (EoS) anteriores al 30/09/2025.
5. Segmentar el acceso remoto VPN y reforzar controles de autenticación.

Prioridad: Crítica

Ampliar Información:

- https://www.tenable.com/blog/cve-2025-20333-cve-2025-20362-faq-cisco-asa-ftd-zero-days-uat4356
- https://www.euskadi.eus/gobierno-vasco/-/noticia/2025/vulnerabilidades-criticas-con-explotacion-activa-en-cisco-secure-firewall-asa-fmc-y-ftd/
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-9
- https://www.ccn-cert.cni.es/es/seguridad-al-dia/alertas-ccn-cert/13100-ccn-cert-al-08-25-campana-de-explotacion-activa-de-tres-vulnerabilidades-criticas-en-dispositivos-cisco-asa-y-ftd.html

CVE-2025-32463 — VULNERABILIDAD CRÍTICA EN SUDO (LINUX/UNIX)

Una vulnerabilidad crítica en la utilidad de línea de comandos Sudo, ampliamente utilizada en sistemas Linux y Unix, está siendo explotada activamente en entornos reales. Este fallo permite a atacantes locales escalar privilegios y ejecutar comandos con permisos de root, incluso sin estar en el archivo *sudoers*.

Resumen técnico:

- CVE-2025-32463 (CVSS 9.3, Crítica): la falla radica en un manejo inseguro de la opción -R (--chroot). Un atacante puede engañar a Sudo para cargar una biblioteca o configuración arbitraria en un directorio controlado, obteniendo así acceso total al sistema.
- Productos afectados: versiones de Sudo entre 1.8.8 y 1.8.32, y entre 1.9.0 y 1.9.17.

- Método de explotación: manipulación de la opción --chroot en combinación con ficheros como nsswitch.conf, lo que permite evadir validaciones y ejecutar comandos arbitrarios.
- Evidencia de explotación: la vulnerabilidad ha sido añadida al catálogo KEV de CISA, confirmando actividad maliciosa activa y presencia de exploits públicos (PoC).

Impacto potencial:

- Compromiso total de estaciones de trabajo y servidores Linux/Unix afectados.
- Posibilidad de robo de información sensible, instalación de malware y establecimiento de persistencia.
- Aumento de la superficie de ataque en entornos corporativos y críticos, dado que Sudo es una utilidad estándar presente en casi todos los sistemas Unix-like.

Recomendaciones de mitigación:

1. Actualizar Sudo a la versión 1.9.17p1 o superior, donde se corrige la vulnerabilidad.
2. Para entornos donde no sea posible actualizar inmediatamente:
3. Deshabilitar la opción -R con Defaults !use_chroot en el archivo /etc/sudoers.
4. Monitorear registros de auditoría (/var/log/auth.log) para detectar intentos de uso sospechoso de sudo con parámetros --chroot.
5. Consultar el catálogo KEV de CISA y priorizar este parche en el plan de gestión de vulnerabilidades.

Prioridad: Crítica.

Ampliar Información:

- https://www.yorku.ca/uit/2025/07/sudo-vulnerability-cve-2025-32463/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-sudo-para-linux-unix-permite-escalada-de-privilegios-locales/
- https://unaaldia.hispasec.com/2025/09/cisa-alerta-vulnerabilidad-critica-en-sudo-permite-escalada-local-a-root.html
- https://blog.segu-info.com.ar/2025/09/fallas-criticas-en-sudo-explotadas.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000
- https://thehackernews.com/2025/09/cisa-sounds-alarm-on-critical-sudo-flaw.html

MALWARE

EVILAI — MALWARE DISFRAZADO DE HERRAMIENTAS DE IA

Investigadores de Trend Micro han identificado una campaña global en la que actores maliciosos distribuyen aplicaciones que aparentan ser herramientas legítimas de inteligencia artificial o productividad, pero que en realidad instalan malware en los sistemas de las víctimas. La campaña, bautizada como EvilAI, afecta a sectores como manufactura, gobierno, salud, tecnología y comercio minorista en regiones de Europa, América, Asia, Oriente Medio y África.

Resumen técnico:

- Los atacantes emplean aplicaciones aparentemente útiles —como AppSuite, Epi Browser, JustAskJacky, Manual Finder, OneStart, PDF Editor, Recipe Lister y Tampered Chef— que cuentan con interfaces profesionales y certificados digitales válidos, dificultando su detección.
- Estas aplicaciones maliciosas realizan reconocimiento del sistema, robo de datos sensibles del navegador, y establecen comunicación cifrada mediante canales AES con servidores C2, permitiendo la descarga de cargas adicionales.
- Se han observado técnicas de firma digital fraudulenta con certificados emitidos en Panamá, Malasia, Ucrania y Reino Unido; así como el uso de NeutralinoJS y homoglifos Unicode para evadir defensas.
- El malware identificado incluye variantes conocidas como BaoLoader y TamperedChef, que comparten infraestructura y operan bajo un posible modelo de malware-as-a-service (MaaS).

Impacto potencial:

- Acceso inicial y persistencia en entornos corporativos mediante software aparentemente legítimo.
- Riesgo de exfiltración de información confidencial, robo de credenciales y espionaje industrial.
- Posibilidad de movimiento lateral y despliegue de ransomware en fases posteriores.
- Compromiso de la cadena de suministro si las aplicaciones se distribuyen a través de portales clonados o marketplaces.

Recomendaciones de mitigación:

1. Validar la procedencia y firma digital de aplicaciones antes de su instalación.
2. Restringir la instalación de software no autorizado y aplicar políticas de principio de mínimo privilegio.

3. Reforzar controles de proxy, descargas y listas blancas para bloquear instaladores no verificados.
4. Utilizar EDR/NGAV con detección basada en comportamiento, monitoreando procesos inusuales, creación de servicios, o conexiones externas anómalas.
5. Revisar segmentación de red y control de egress, aplicando inspección TLS donde sea posible.
6. Concienciar a usuarios sobre los riesgos de instalar herramientas de IA/productividad no verificadas.

Prioridad: Importante.

Ampliar Información:

- https://qsecure.es/evilai-malware-que-se-hace-pasar-por-herramientas-de-ia-para-infiltrarse-en-organizaciones-globales/
- https://thehackernews.com/2025/09/evilai-malware-masquerades-as-ai-tools.html
- https://www.softonic.com/articulos/la-campana-evilai-aprovecha-aplicaciones-de-confianza-para-propagar-software-malicioso#google_vignette
- https://blog.tecnetone.com/detectan-malware-evilai-disfrazado-de-herramienta-de-ia?hs_amp=true

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

CONFUCIUS HACKERS DESPLIEGA WOOPERSTEALER Y ANONDOOR EN CAMPAÑA CONTRA PAKISTÁN

El grupo de ciberespionaje Confucius, activo desde 2013 y con historial de operaciones en el sur de Asia, ha sido vinculado a una nueva campaña dirigida contra entidades gubernamentales, militares y de defensa en Pakistán.

Resumen técnico:

- Vector inicial: campañas de spear-phishing mediante documentos maliciosos .PPSX y accesos directos .LNK.
- Carga útil: uso de DLL side-loading para desplegar WooperStealer y, en fases posteriores, el backdoor en Python Anondoor.
- Capacidades de WooperStealer: robo de credenciales, exfiltración de datos sensibles, captura de información del sistema y pantallazos.
- Infraestructura: servidores externos controlados por el actor, rotación de dominios y técnicas de ofuscación para evadir detección.

Impacto potencial:

- Compromiso de entidades gubernamentales y de defensa con fines de espionaje estratégico.

- Robo de credenciales y datos sensibles que pueden facilitar movimientos laterales dentro de la red.
- Persistencia a largo plazo con capacidad de ampliar el alcance a sectores críticos.
- Dificultad de detección por el uso de técnicas de side-loading y herramientas personalizadas.

Recomendaciones para mitigar el riesgo:

- Seguridad en endpoints: bloquear DLL side-loading, aplicar políticas WDAC/AppLocker y reforzar EDR para detectar comportamientos anómalos.
- Control de correo: fortalecer filtros antiphishing y aplicar sandboxing para archivos adjuntos sospechosos (.PPSX, .LNK).
- Gestión de credenciales: rotar contraseñas críticas y habilitar MFA resistente a phishing.
- Monitorización de red: analizar tráfico sospechoso hacia dominios y C2 desconocidos.
- Concienciación: entrenar usuarios en detección de correos maliciosos y documentos sospechosos.
- Threat hunting: buscar indicadores asociados a WooperStealer y Anondoor, así como artefactos de persistencia.

Prioridad: Importante.

Ampliar Información:

- https://thehackernews.com/2025/10/confucius-hackers-hit-pakistan-with-new.html