GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º5225

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	2	1	0
MALWARE	1	0	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

CISCO SECURE EMAIL GATEWAY — VULNERABILIDAD ZERO-DAY CRÍTICA EXPLOTADA ACTIVAMENTE (CVE-2025-20393)

Se ha detectado una campaña de ciberespionaje avanzada (APT) por parte del actor UAT-9686 (vinculado a China) dirigida contra dispositivos Cisco Secure Email Gateway y Secure Email and Web Manager. Los atacantes explotan una vulnerabilidad zero-day crítica que permite la ejecución remota de comandos con privilegios de root sin necesidad de autenticación previa.

Resumen técnico:

- Identificador principal: CVE-2025-20393 (Zero-day, incluido en el catálogo KEV de CISA).
- Severidad: 10.0 (Crítica).
- Estado: Explotación activa confirmada desde finales de noviembre de 2025.
- Causa raíz: Validación inadecuada de entradas en el software AsyncOS.
- Condición de explotación: La interfaz de Spam Quarantine debe estar habilitada y expuesta directamente a Internet (configuración no recomendada).
- Versiones afectadas: Todas las versiones de Cisco AsyncOS que ejecuten Secure Email Gateway o Secure Email and Web Manager bajo la condición de exposición mencionada.

Impacto potencial:

- Control total (root) del appliance de seguridad perimetral.
- Exfiltración e interceptación de comunicaciones corporativas sensibles.
- Persistencia mediante la instalación de implantes personalizados (backdoors).
- Pivoteo y movimiento lateral hacia la red interna de la organización.

Recomendaciones de mitigación:

1. Actualización de emergencia: Aplicar los parches de seguridad provistos por Cisco de forma inmediata.
2. Restricción de exposición: Eliminar o limitar el acceso a la interfaz de Spam Quarantine desde Internet, utilizando VPN o listas de confianza.
3. Reconstrucción de activos: En caso de confirmarse un compromiso, se recomienda la reconstrucción completa del appliance para asegurar la eliminación de la persistencia.
4. Monitoreo: Revisar logs en busca de solicitudes HTTP POST inusuales y anomalías en el borrado de registros.

Prioridad: Crítica.

Ampliar información:

- https://unaaldia.hispasec.com/2025/12/cve-2025-20393-explotacion-activa-en-cisco-asyncos-permite-ejecutar-comandos-con-privilegios-root.html
- https://www.integrity360.com/es/cyber-news-roundup-december-19th-2025
- https://socprime.com/es/blog/cve-2025-20393-vulnerability-exploitation/
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/2403

PLACAS BASE (ASUS, GIGABYTE, MSI, ASROCK) — FALLO EN IMPLEMENTACIÓN UEFI PERMITE ATAQUES DMA (CVE-2025-11901 Y OTROS)

Investigadores de Riot Games han descubierto una vulnerabilidad crítica en el firmware UEFI de los principales fabricantes de placas base. El fallo, denominado como "Sleeping Bouncer", permite que dispositivos PCIe maliciosos realicen ataques de Acceso Directo a la Memoria (DMA) antes de que el sistema operativo se inicie, invalidando las protecciones de seguridad del kernel.

Resumen técnico:

- Identificadores: CVE-2025-11901 (ASUS), CVE-2025-14302 (GIGABYTE), CVE-2025-14303 (MSI), CVE-2025-14304 (ASRock).
- Severidad: 7.0 (Alta).
- Causa raíz: Discrepancia en el estado de protección DMA. El firmware informa erróneamente que la protección está activa cuando la IOMMU (Unidad de Gestión de Memoria de Entrada-Salida) no ha sido inicializada correctamente en la fase crítica de arranque.
- Versiones afectadas: Modelos con chipsets Intel (series 400 a 800) y AMD (series X670, B650, X870, entre otros).

Impacto potencial:

- Inyección de código malicioso antes del arranque del sistema operativo (bootkits).
- Bypass de soluciones de seguridad que funcionan a nivel de kernel (como Vanguard o sistemas EDR).
- Exposición de claves de cifrado y credenciales almacenadas en la memoria RAM.
- Acceso persistente y casi indetectable por herramientas de software tradicionales.

Recomendaciones de mitigación:

1. Actualización de Firmware: Aplicar de forma inmediata las actualizaciones de BIOS/UEFI proporcionadas por el fabricante de la placa base.
2. Control Físico: Restringir el acceso físico a los equipos para evitar la conexión de dispositivos PCIe o Thunderbolt maliciosos.
3. Seguridad de Puertos: En entornos de alta seguridad, deshabilitar puertos externos de alta velocidad si no son estrictamente necesarios para la operación.

Prioridad: Urgente.

Ampliar información:

- https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/nueva-vulnerabilidad-de-uefi-permite-ataques-dma-de-arranque-temprano-en-placas-base-asrock-asus-gigabyte-y-msi/
- https://global.techradar.com/es-mx/pro/security/las-placas-base-de-gigabyte-msi-asus-y-asrock-corren-peligro-por-un-nuevo-ataque-de-vulnerabilidad-uefi-esto-es-lo-que-sabemos
- https://blog.segu-info.com.ar/2025/12/fallos-en-uefi-permiten-ataques-en.html

N8N — VULNERABILIDAD CRÍTICA DE EJECUCIÓN REMOTA DE CÓDIGO (CVE-2025-68613)

Se ha reportado una falla de máxima severidad en la popular plataforma de automatización de flujos de trabajo n8n. Debido a que estas herramientas suelen centralizar credenciales sensibles y conectar múltiples servicios corporativos (APIs, bases de datos, CRMs), una explotación exitosa podría resultar en un compromiso total de la infraestructura de automatización.

Resumen técnico:

- Identificador principal: CVE-2025-68613.
- Severidad: 9.9 / 10.0 (Crítica).
- Causa raíz: Aislamiento insuficiente (sandboxing) en el sistema de evaluación de expresiones. Ciertas expresiones suministradas por usuarios no son filtradas correctamente antes de ser evaluadas por el runtime.
- Vector de ataque: Un atacante autenticado puede inyectar código arbitrario durante la configuración de un flujo de trabajo, ejecutándolo con los privilegios del proceso n8n.
- Versiones afectadas: Todas las versiones desde la 0.211.0 hasta versiones anteriores a la 1.120.4.

Impacto potencial:

- Ejecución de comandos arbitrarios en el servidor subyacente (RCE).
- Acceso no autorizado a secretos, claves de API y datos sensibles gestionados en otros flujos de trabajo.
- Modificación o alteración de automatizaciones críticas del negocio.
- Capacidad de realizar movimientos laterales hacia otros sistemas conectados a la plataforma.

Recomendaciones de mitigación:

1. Actualización obligatoria: Actualizar n8n a las versiones 1.120.4, 1.121.1, 1.122.0 o superiores de forma inmediata.
2. Gestión de privilegios: Restringir los permisos de creación y edición de flujos de trabajo únicamente a personal de absoluta confianza (Principio de Menor Privilegio).
3. Aislamiento de red: Desplegar n8n en entornos endurecidos (hardened) con privilegios de sistema operativo restringidos y acceso de red limitado a lo estrictamente necesario.

Prioridad: Crítica.

Ampliar información:

- https://csirt.telconet.net/comunicacion/noticias-seguridad/nueva-vulnerabilidad-critica-de-ejecucion-remota-de-codigo-rce-con-puntuacion-cvss-10-que-afecta-a-n8n-cve-2025-68613/
- https://cibersafety.com/vulnerabilidad-cve-ejecucion-remota-n8n/
- https://devel.group/blog/mas-de-100000-instancias-de-n8n-expuestas-a-ejecucion-remota-de-codigo-rce/
- https://thehackernews.com/2025/12/critical-n8n-flaw-cvss-99-enables.html

MALWARE

CRYPTO24 — RANSOMWARE DE DOBLE EXTORSIÓN CON EVASIÓN AVANZADA DE EDR

Se ha identificado una campaña coordinada del ransomware Crypto24 con un fuerte enfoque en organizaciones de América Latina, Asia y EE. UU. Este actor de amenazas destaca por su madurez operativa, utilizando técnicas de "Living-off-the-Land" (LotL) y herramientas personalizadas para neutralizar defensas modernas y evadir la detección de sistemas EDR.

Resumen técnico:

- Tipo de amenaza: Ransomware de doble extorsión.
- Técnica de evasión: Utiliza una versión personalizada de RealBlindingEDR, diseñada específicamente para desinstalar o desactivar productos de seguridad (como Sophos, Bitdefender, Kaspersky y Microsoft Defender) mediante el uso indebido de controladores legítimos.
- Persistencia y Movimiento Lateral: Aprovecha procesos legítimos como svchost.exe y tareas programadas. Utiliza herramientas como PSExec, AnyDesk y comandos estándar de Windows (net.exe) para crear cuentas privilegiadas y moverse por la red.
- Exfiltración: Emplea una herramienta propia basada en la API WinINET para transferir datos robados directamente a Google Drive de forma sigilosa.
- Ofuscación: El binario está protegido con la virtualización VMProtect para dificultar la ingeniería inversa y el análisis forense.

Impacto potencial:

- Doble Extorsión: Cifrado de archivos (extensión .crypto24) combinado con la amenaza de publicar información sensible en la Dark Web.
- Inhabilitación de Defensas: Compromiso total del endpoint al dejarlo sin protección antivirus/EDR activa antes del despliegue del ransomware.
- Pérdida de Continuidad: Eliminación de Shadow Copies (instantáneas de volumen) para impedir la recuperación de datos sin el pago del rescate.

Recomendaciones de mitigación:

1. Control de Cuentas: Auditar y limitar la creación de cuentas administrativas locales y deshabilitar perfiles predeterminados no utilizados.
2. MFA y RDP: Implementar autenticación multifactor (MFA) obligatoria y restringir el uso de RDP y herramientas de acceso remoto (AnyDesk, PsExec) solo a hosts autorizados.
3. Monitoreo de Herramientas LotL: Vigilar ejecuciones inusuales de wmic.exe, psexec.exe y scripts .bat en directorios temporales o de sistema (%ProgramData%).
4. Principio de Menor Privilegio: Asegurar que los usuarios operen con permisos mínimos, ya que el desinstalador de EDR requiere privilegios de administrador para funcionar.

Prioridad: Crítica.

Ampliar información:

- https://www.hendryadrian.com/ransom-unified-assessment-platform-examroom-ai/
- https://www.hookphish.com/blog/ransomware-group-crypto24-hits-unified-assessment-platform-examroom-ai/
- https://blog.segu-info.com.ar/2025/12/ransomware-crypto24-activo-en-america.html

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

MICROSOFT RETIRARÁ EL CIFRADO RC4 DE WINDOWS PARA REFORZAR LA AUTENTICACIÓN KERBEROS

Microsoft ha anunciado formalmente que dejará de dar soporte al algoritmo de cifrado RC4 en los procesos de autenticación vía Kerberos dentro de Windows Server. Esta medida, prevista para consolidarse a mediados de 2026, busca eliminar una de las vías más comunes utilizadas por atacantes para el robo de credenciales y el movimiento lateral en redes corporativas.

Resumen técnico:

- Contexto: El cifrado RC4 (Rivest Cipher 4), introducido hace más de 25 años, ha sido el método predeterminado en Active Directory para proteger componentes críticos, a pesar de sus debilidades conocidas.
- Actualización: El Centro de Distribución de Claves Kerberos (KDC) en Windows Server 2008 y versiones posteriores se configurará para permitir únicamente el cifrado AES-SHA1 (mucho más robusto y lento de descifrar).
- Vulnerabilidad principal: RC4 carece de "salts" criptográficos y utiliza una implementación débil de MD4, lo que facilita ataques de Kerberoasting (Mitre ATT&CK T1558-003) para descifrar contraseñas de cuentas de servicio sin conexión.
- Transición: Microsoft deshabilitará RC4 de forma predeterminada, permitiendo su uso únicamente si un administrador lo configura de manera explícita para sistemas heredados.

Impacto potencial:

- Reducción drástica del riesgo de compromiso de identidad y acceso no autorizado mediante técnicas de fuerza bruta.
- Posibles interrupciones en sistemas de terceros o infraestructuras muy antiguas que dependan exclusivamente de RC4 para autenticarse.
- Elevación de los estándares de cumplimiento y blindaje corporativo en entornos de Active Directory.

Recomendaciones para mitigar el riesgo:

1. Auditoría de red: Utilizar los nuevos scripts de PowerShell proporcionados por Microsoft para identificar sistemas que aún dependen de RC4.
2. Monitoreo de KDC: Habilitar el registro de eventos del KDC para rastrear solicitudes de autenticación basadas en RC4 antes de que llegue la fecha límite.
3. Migración a AES: Reconfigurar las cuentas de servicio y los controladores de dominio para forzar el uso de AES-128/256.
4. Pruebas de interoperabilidad: Verificar la compatibilidad de aplicaciones críticas de terceros antes del despliegue masivo de las nuevas políticas en 2026.

Prioridad: Importante.

Ampliar Información:

- https://www.diariotecnologia.es/posts/el-fin-de-una-era-microsoft-jubila-el-cifrado-rc4-tras-25-aos-y-mltiples-vulnerabilidades
- https://blog.segu-info.com.ar/2025/12/microsoft-finalmente-elimina-el-cifrado.html
- https://www.infobae.com/america/agencias/2025/12/16/microsoft-retirara-el-cifrado-rc4-de-windows-para-reforzar-la-seguridad-de-los-inicios-de-sesion-tras-varias-brechas/