Boletín informativo
Vulnerabilidades críticas en Apple

CSIRTSALUD-AV-20260309-34 **TLP: CLEAR**

Incidente ID:	034
Fecha del reporte:	09/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidades críticas en Apple
Herramienta de detección	N/A
Activo involucrado:	macOS, iOS, iPadOS, Safari, tvOS, watchOS
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema sobre tres vulnerabilidades críticas en productos Apple (macOS, iOS, iPadOS, Safari, tvOS y watchOS) que han sido incorporadas por la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) al catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el día 5 de marzo de 2026.

Las fallas están siendo aprovechadas activamente por actores de amenaza en campañas de ciber espionaje y robo de criptoactivos mediante el kit de explotación conocido como "Coruna". La divulgación de esta alerta busca promover la aplicación inmediata de los parches de seguridad disponibles y fortalecer las capacidades de detección y respuesta ante incidentes en entornos corporativos y personales.

Descripción:

El 5 de marzo de 2026, CISA añadió tres fallas de seguridad al catálogo KEV tras confirmar su explotación activa por parte de actores de amenaza sofisticados. Las vulnerabilidades se concentran en WebKit (motor de navegación de Safari utilizado por todos los navegadores de iOS) y afectan componentes de administración de memoria en múltiples versiones del ecosistema Apple.

Kit de explotación: Coruna

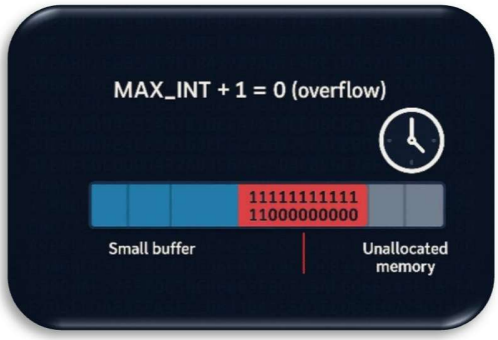
La explotación de estas vulnerabilidades está vinculada al kit de explotación denominado "Coruna", una herramienta inicialmente desarrollada para operaciones de vigilancia estatal y que posteriormente fue comercializada en el mercado negro de exploits. Las investigaciones de inteligencia de amenazas indican que este kit migró desde actores de vigilancia de origen estadounidense hacia grupos de actores patrocinados por estados y, más recientemente, a organizaciones criminales de origen chino especializadas en robo de criptoactivos.

El fenómeno de "reciclaje de zero-days" observado en este caso muestra cómo exploits desarrollados por inteligencia estatal terminan siendo reutilizados por cibercriminales años después de su descubrimiento.

Las tres vulnerabilidades corresponden a errores de gestión de memoria y aritmética de enteros que permiten a atacantes remotos ejecutar código arbitrario en el dispositivo víctima, incluyendo en algunos casos la obtención de privilegios de nivel kernel (raíz del sistema operativo).

Explicación de las Vulnerabilidades Parchadas

- **CVE-2021-30952 (Integer Overflow):** Un fallo en el manejo de memoria que ocurre cuando el sistema procesa contenido web malicioso. Al exceder el límite numérico de una variable, el atacante provoca un comportamiento inesperado que permite la ejecución de código.



- **CVE-2023-41974 (Use-After-Free):** Una vulnerabilidad en la que una aplicación accede a una dirección de memoria después de que esta ha sido liberada. Esto permite a un atacante ejecutar código arbitrario con **privilegios de kernel**, el nivel más alto del sistema.

- **CVE-2023-43000 (Use-After-Free en WebKit):** Afecta al motor de renderizado de Safari. Al procesar contenido web diseñado maliciosamente, se produce una corrupción de memoria que facilita la toma de control del proceso del navegador.

La explotación exitosa de estas vulnerabilidades puede derivar en consecuencias de alto impacto tanto para usuarios individuales como para organizaciones:

- **Ejecución de código arbitrario:** El atacante puede ejecutar código malicioso con los privilegios del usuario o del kernel, tomando control total del dispositivo.

- **Corrupción de memoria (Memory Corruption):** Modifica zonas de memoria del sistema operativo para alterar el flujo de ejecución de procesos críticos.
- **Escalamiento de privilegios hasta nivel kernel:** Permite acceso irrestricto a todas las funciones del sistema operativo, eludiendo sandboxes y mecanismos de seguridad.
- **Instalación de spyware persistente:** Los actores de amenaza han aprovechado el acceso conseguido para instalar herramientas de vigilancia similares a Pegasus, permitiendo captura de mensajes, llamadas, geolocalización y contraseñas.
- **Compromiso completo del dispositivo:** Acceso a datos personales, contraseñas, billeteras de criptomonedas, correos electrónicos, documentos sensibles y cámaras/micrófonos.
- Filtración de información corporativa confidencial e inteligencia empresarial.
- Robo de credenciales de acceso a sistemas críticos (VPN, correo, ERP).
- **Compromiso de dispositivos de alto perfil:** directivos, periodistas, activistas y funcionarios gubernamentales.
- Pérdida de criptoactivos en plataformas de intercambio y billeteras digitales.

Productos afectados:

Aquí está el listado completo de activos afectados, cruzado con cada vulnerabilidad:

Activo / Producto	Versión Vulnerable	CVE-2023-43000	CVE-2021-30952	CVE-2023-41974	Versión Corregida
iOS (iPhone 8 y posteriores)	Anterior a 18.1	☑	☑	☑	iOS 18.1
iOS 16 (iPhone 8, X; iPad 5ta–7ta gen, mini 5ta, Air 3ra)	Anterior a 16.7.2	☑	☑	☑	iOS 16.7.2
iOS 15 (iPhone 6s, 7, SE 1ra gen; iPod touch 7ta gen)	Anterior a 15.8.1	☑	☑	☑	iOS 15.8.1
iPadOS (iPad 5ta generación y posteriores)	Anterior a 18.1	☑	☑	☑	iPadOS 18.1
iPadOS 16	Anterior a 16.7.2	☑	☑	☑	iPadOS 16.7.2
iPadOS 15 (iPad Air 2, iPad mini 4ta gen)	Anterior a 15.8.1	☑	☑	☑	iPadOS 15.8.1

Activo / Producto	Versión Vulnerable	CVE-2023-43000	CVE-2021-30952	CVE-2023-41974	Versión Corregida
macOS Sonoma	Anterior a 14.1	☑	☑	✗	macOS Sonoma 14.1
macOS Ventura	Anterior a 13.6.1	☑	☑	✗	macOS Ventura 13.6.1
macOS Monterey	Anterior a 12.7.1	☑	☑	✗	macOS Monterey 12.7.1
Safari	Anterior a 17.1	☑	☑	✗	Safari 17.1
tvOS	Anterior a 17.1	✗	☑	✗	tvOS 17.1
watchOS	Anterior a 10.1	✗	☑	✗	watchOS 10.1

Notas clave:

- **CVE-2023-41974** es la única que impacta **exclusivamente iOS/iPadOS** — es la más crítica porque permite el escalamiento a kernel.
- **CVE-2021-30952** es la de mayor alcance, afectando hasta **watchOS y tvOS**.
- **CVE-2023-43000** afecta todos los dispositivos con Safari 16.6, incluyendo macOS.
- Los dispositivos **iOS/iPadOS son los únicos expuestos a las tres vulnerabilidades simultáneamente**, lo que los convierte en el vector de ataque más crítico.

Modo de explotación y cadena de infección

La cadena de explotación documentada sigue un patrón de ataque en múltiples etapas (multi-stage attack chain) que combina las tres vulnerabilidades para lograr un compromiso completo y persistente del dispositivo objetivo.

Fase 1 — Entrega y punto de entrada (Initial Access)

El atacante prepara una página web especialmente diseñada (malicious landing page) alojada en infraestructura controlada. El vector de entrega puede ser:

- Correo electrónico de spear-phishing con enlace malicioso dirigido a personas de interés específico.

- Mensaje SMS/iMessage con enlace (smishing) hacia la página trampa.
- Ataque de tipo watering hole en sitios legítimos frecuentados por el objetivo.
- Inyección de contenido web en redes Wi-Fi no seguras (man-in-the-middle).

Cuando la víctima accede a la URL maliciosa, el navegador (Safari u otro basado en WebKit en iOS) comienza a procesar el contenido HTML/JavaScript/WebGL diseñado para activar las vulnerabilidades.

Fase 2 — Corrupción de memoria inicial (CVE-2021-30952: Integer Overflow)

El exploit aprovecha el desbordamiento de enteros en el motor de renderizado WebKit para crear una condición donde el buffer asignado es insuficiente para el contenido procesado. Al procesar contenido web malicioso con estructuras de objetos JavaScript de tamaño calculado específicamente, el motor crea una aritmética de enteros que produce un valor demasiado grande para el espacio de almacenamiento asignado.

Esta condición genera una escritura fuera de límites (out-of-bounds write) que corrompe zonas de memoria adyacentes. El atacante utiliza heap-spraying (rociado del heap) para posicionar su shellcode en las posiciones de memoria que serán sobreescritas, preparando el terreno para la siguiente etapa.

Fase 3 — Ejecución de código arbitrario (CVE-2023-43000: Use-After-Free)

Con la memoria del heap ya preparada, el exploit activa la vulnerabilidad Use-After-Free (UAF) en el componente de renderizado de macOS, iOS, iPadOS y Safari 16.6. En una vulnerabilidad UAF, el programa libera un objeto de memoria pero mantiene un puntero (referencia) a esa zona liberada.

El atacante manipula el flujo de ejecución de JavaScript para: (1) asignar un objeto en el heap, (2) forzar su liberación prematura, (3) rellenar la zona de memoria liberada con datos controlados por el atacante, y (4) forzar el uso del puntero obsoleto. Cuando el motor WebKit intenta acceder al objeto ya liberado, en realidad accede a los datos del atacante, permitiendo redirigir el flujo de ejecución hacia el shellcode posicionado en la Fase 2.

El resultado es la ejecución de código arbitrario en el contexto del proceso del navegador (renderer process), obteniendo un shell dentro de la sandbox del navegador con los privilegios del usuario.

Fase 4 — Escalamiento de privilegios a nivel kernel (CVE-2023-41974: Use-After-Free)

A partir del acceso obtenido en el contexto del renderer, el exploit encadena la segunda vulnerabilidad UAF (CVE-2023-41974) que afecta exclusivamente a iOS y iPadOS. Esta falla reside en la comunicación entre el proceso del navegador y el proceso privilegiado del sistema (kernel).

Una aplicación maliciosa (o el código ya ejecutado en el navegador) puede invocar una secuencia de operaciones que provoca una condición use-after-free en el espacio del kernel, permitiendo escritura en zonas de memoria protegidas del sistema operativo. Esto otorga al

atacante privilegios de nivel kernel (ring 0), eludiendo completamente los mecanismos de sandboxing, Pointer Authentication Codes (PAC) y otros controles de seguridad de Apple.

Fase 5 — Post-explotación y persistencia

Con privilegios de kernel, el atacante procede a instalar el payload final, que en las campañas documentadas incluye:

- Implantación de un agente de vigilancia persistente similar a Pegasus, capaz de sobrevivir reinicios mediante modificación de la partición del sistema.
- Extracción silenciosa del keychain de iOS/macOS con todas las contraseñas almacenadas, incluyendo seed phrases de billeteras de criptomonedas.
- Activación de acceso remoto al micrófono, cámara y GPS del dispositivo.
- Exfiltración de mensajes (iMessage, WhatsApp, Signal) mediante hooks al proceso de mensajería.
- Establecimiento de canal de comunicación cifrado (C2) hacia la infraestructura controlada por el atacante.

Relación con Tácticas MITRE ATT&CK

El comportamiento observado se alinea con las siguientes tácticas de la matriz MITRE:

Táctica	Técnica ID	Descripción
Acceso Inicial	[T1189]	Drive-by Compromise (vía sitios web infectados).
Ejecución	[T1203]	Exploitation for Client Execution (WebKit).
Escalada de Privilegios	[T1068]	Exploitation for Privilege Escalation (Fallas de Kernel).
Evasión de Defensas	[T1548]	Abuse Elevation Control Mechanism.
Exfiltración	[T1020]	Automated Exfiltration (Robo de billeteras).

Indicadores de compromiso:

Los indicadores de compromiso son artefactos observables que, con alta probabilidad, indican actividad maliciosa relacionada con la explotación de estas vulnerabilidades. Los IoC asociados al kit Coruna y campañas relacionadas incluyen:

Comportamientos del sistema (Behavioral IoC)

- Procesos inusuales lanzados por WebKit o Safari que generan subprocesos con privilegios elevados.
- Llamadas al sistema operativo (syscalls) inusuales desde el proceso del navegador, especialmente mmap(), mprotect() y vm_allocate().
- Escrituras inesperadas en regiones de memoria del kernel desde el espacio de usuario.
- Acceso no autorizado al micrófono, cámara o GPS sin intervención del usuario.
- Conexiones de red salientes hacia dominios/IPs no reconocidos después de visitar páginas web.
- Crash Reports frecuentes en WebKit (archivo .crash en /Library/Logs/DiagnosticReports/).
- Aparición de perfiles de configuración desconocidos en Ajustes > General > Gestión de dispositivos.

Artefactos de red

- Tráfico HTTPS hacia dominios con certificados auto-firmados o de reciente creación (< 30 días).
- Conexiones persistentes tipo beaconing con intervalos regulares a IPs en rangos no asociados a servicios legítimos de Apple.
- Exfiltración de datos mediante canales encubiertos (DNS-over-HTTPS, HTTP/2 con padding).

Artefactos de archivos

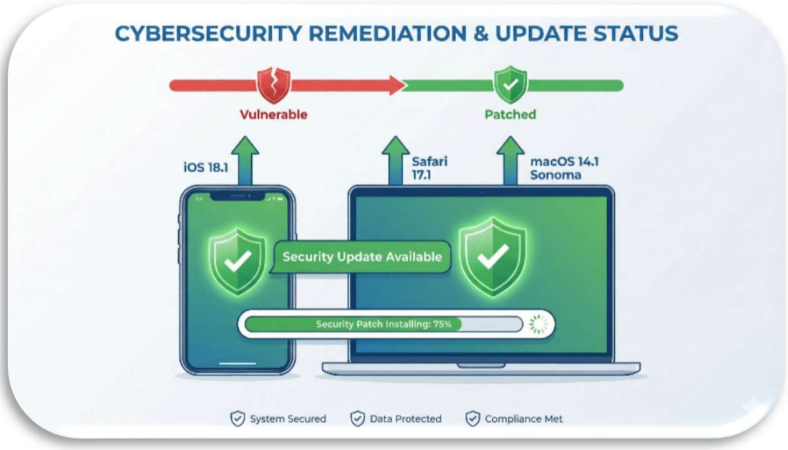
- Archivos .dylib no firmados en directorios del sistema (/usr/lib/, /Library/Frameworks/).
- Modificaciones no autorizadas en /etc/hosts o en perfiles de configuración de red.
- Presencia de binarios con nombres genéricos (update, helper, sync) en /tmp/ o ~/Library/Caches/.

Recomendaciones de mitigación:

La única remediación definitiva es la aplicación de los parches de seguridad oficiales de Apple. Se deben actualizar todos los dispositivos Apple a las versiones que incluyen las correcciones:

- iOS y iPadOS 18.1 o superior (para dispositivos iPhone 8 / iPad 5ta gen o más recientes).
- iOS 16.7.2+ e iOS 15.8.1+ para dispositivos más antiguos (iPhone 6s, 7, SE 1ra gen, iPad Air 2, iPad mini 4ta gen).
- macOS Sonoma 14.1, macOS Ventura 13.6.1 y macOS Monterey 12.7.1 o versiones superiores.
- tvOS 17.1+, watchOS 10.1+ y Safari 17.1+ en macOS compatible.

Para actualizar: Ajustes > General > Actualización de Software (iOS/iPadOS) | Preferencias del Sistema > Actualización de Software (macOS).



Detección de Actividad Maliciosa

Para detectar posibles compromisos derivados de estas vulnerabilidades, se recomienda:

- Revisar Crash Reports de WebKit/Safari: Acceder a Ajustes > Privacidad > Análisis y mejoras > Datos de análisis para identificar crashes frecuentes en procesos WebKit.

- Monitorear conexiones de red inusuales: Usar herramientas como Little Snitch (macOS) o iShutdown (iOS) para identificar conexiones salientes no autorizadas desde Safari o procesos del sistema.
- Auditar perfiles de configuración instalados: Ajustes > General > VPN y gestión de dispositivos. Eliminar cualquier perfil no reconocido o no instalado intencionalmente.
- Verificar integridad de aplicaciones: En entornos empresariales, revisar el MDM (Mobile Device Management) para detectar aplicaciones no autorizadas o perfiles maliciosos.
- Implementar reglas YARA/Sigma: Desarrollar o importar reglas de detección para patrones de heap-spray, shellcode en procesos de WebKit y conexiones C2 de balizamiento.
- Revisar logs del sistema (macOS): Usar Console.app o el comando log stream --predicate 'process == "Safari"' para monitorear actividad anómala del navegador.
- Análisis de tráfico de red: Implementar inspección TLS en perímetro corporativo para detectar comunicaciones C2 con certificados inusuales o hacia dominios de baja reputación.

Medidas de Hardening Preventivo

- Activar el modo de aislamiento (Lockdown Mode) en iOS 16+ para usuarios de alto riesgo: reduce drásticamente la superficie de ataque, aunque limita algunas funcionalidades.
- Restringir JavaScript en Safari para sitios no confiables: Ajustes > Safari > Avanzado (activar con precaución, puede afectar la navegación).
- Implementar un Content Security Policy (CSP) robusto en servidores web corporativos para dificultar la entrega de exploits vía web.
- Usar DNS con filtrado de dominios maliciosos (Cisco Umbrella, NextDNS, Pi-hole) para bloquear la resolución de dominios C2 conocidos.
- Habilitar autenticación multifactor (MFA) en todas las cuentas de Apple ID y servicios corporativos, para limitar el impacto de credenciales robadas.

- Establecer política de actualización forzada en entornos MDM/EMM (Jamf, Intune) con ventanas de actualización automática de máximo 24 horas después de disponibilidad del parche.
- Realizar ejercicios de threat hunting periódicos enfocados en IoC relacionados con WebKit, Safari y procesos de sistema en dispositivos Apple.

Fuentes:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://support.apple.com/en-us/HT213938
- https://nvd.nist.gov/vuln/detail/CVE-2023-43000
- https://nvd.nist.gov/vuln/detail/CVE-2023-41974
- https://nvd.nist.gov/vuln/detail/CVE-2021-30952
- https://attack.mitre.org/
- https://www.cisecurity.org/benchmark/apple_os
- https://www.cisa.gov/news-events/directives/bod-22-01
- https://www.bleepingcomputer.com/news/security/cisa-warns-of-apple-flaws-exploited-in-spyware-crypto-theft-attacks/#:~:text=The%20U.S.%20Cybersecurity%20and%20Infrastructure%20Security%20Agency,crypto%2Dtheft%20attacks%20using%20the%20Coruna%20exploit%20kit.
- https://socprime.com/blog/cve-2026-20700-vulnerability/#:~:text=Devices%20running%20vulnerable%20versions%2C%20especially%20those%20not,26.3%2C%20and%20macOS%20Tahoe%2026.3%2C%20where%20applicable
- https://www.scworld.com/news/3-apple-flaws-from-coruna-exploit-kit-added-to-cisa-vulnerability-list

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.