Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°163**	**Fecha: 11-07-2023**
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Zero Day de tipo ejecución de código arbitrario en WebKit de Apple		
Tipo de Ataque	Exploits	Abreviatura	Exploits
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Un investigador anónimo ha informado a la compañía Apple de una vulnerabilidad de tipo Zero Day que podría permitir a un atacante ejecutar código arbitrario en equipos iPhones, Mac, y iPads, aunque tengan los parches completos.

Esta amenaza representa un grave riesgo para los usuarios de estos equipos. Por eso, en respuesta, Apple emitió una serie de actualizaciones de respuesta rápida de seguridad para abordar esta amenaza.

2. DETALLES:

La plataforma para aplicaciones WEBKIT se encuentra expuesta a contenido web potencialmente peligroso. Apple ha informado de que esta vulnerabilidad puede haber sido explotada activamente. Se ha asignado el identificador CVE-2023-37450 para esta vulnerabilidad.

Este exploit de día cero permite al atacante ejecutar código arbitrario en dispositivos específicos. Al atraer a los usuarios desprevenidos a páginas web con contenido malicioso, el atacante puede obtener el control, lo que podría generar una cascada de infracciones.

Para contrarrestar este exploit, Apple ha lanzado “Rapid Security Response”, una línea de defensa intermedia que proporciona mejoras de seguridad cruciales entre las actualizaciones regulares de software, la cual podría incluir mejoras en el navegador web Safari, la pila del marco WebKit u otras bibliotecas críticas del sistema.

Los parches de emergencia para las últimas versiones de, iOS, iPadOS y macOS, a partir de iOS 16.4.1, iPadOS 16.4.1 y macOS 13.3.1 son las siguientes: iOS 15.5.1 (a), iPadOS 16.5.1 (a), macOS Ventura 13.4.1 y Safari 16.5.2.

Además, Apple es consciente de que esta respuesta de seguridad rápida podría impedir que algunos sitios web se muestren correctamente. “Rapid Security Response” en iOS 16.5.1 (b) y iPadOS 16.5.1 (b) estarán disponibles pronto para solucionar este problema.

Finalmente, Apple incluirá el parche de seguridad en una futura actualización del software.

A. **Productos afectados:**

- iOS 16.5.1 y iPadOS 16.5.
- MacOS Ventura 13.4.1;
- Safari 16.5.2

3. RECOMENDACIONES:

- Actualizar a las versiones referenciadas siguiendo los pasos indicados en la web oficial del fabricante.
- Personalizar las actualizaciones automáticas en su dispositivo Apple, tal cual está en la fuente de información.

Fuente de Información:	• hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos/0day-de-tipo-ejecucion-de-codigo-arbitrario-en-webkit-de-apple • hxxps://securityonline.info/cve-2023-37450-0-day-bug-affecting-iphones-macs-and-ipads/ • hxxps://support.apple.com/es-es/HT204204

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°163	Fecha: 11-07-2023
		Página: 5 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de infección de malware “Triada” dirigida a dispositivos Android		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Investigadores de Check Point Software Technologies, han reportado una nueva campaña de infección de malware “Triada”, que se distribuye a través de una versión pirateada de la plataforma de mensajería Telegram, en tiendas de terceros en lugar de la tienda oficial de Google. Esta campaña está dirigido a dispositivos con sistema operativo Android.

2. DETALLES:

La versión maliciosa de la aplicación Telegram que contiene el malware “Triada” se oculta hábilmente como la última versión de Telegram Messenger, específicamente la versión 9.2.1. Esta aplicación pirateada no se puede encontrar en Google Play Store, sino en tiendas de aplicaciones de terceros.

Los investigadores indicaron que para hacer que la versión modificada parezca legítima, los atacantes han empleado tácticas como usar un nombre de paquete (org.telegram.messenger), que se parece a la aplicación genuina y utilizar el ícono verificado de la aplicación.

Al iniciar la aplicación maliciosa, se carga una ventana de inicio de sesión que imita perfectamente la página de inicio de la aplicación original. Luego, para continuar con el registro, les solicita a los usuarios que ingresen su número de teléfono y otorguen acceso a los permisos del dispositivo.

A continuación, la aplicación maliciosa inserta código dañino en el dispositivo bajo la apariencia de un servicio interno de actualización de aplicaciones. El malware Triada opera discretamente en segundo plano, recopila información del dispositivo, recupera archivos de configuración y establece canales de comunicación.

De igual forma, el malware también puede inscribir a las víctimas en múltiples suscripciones pagas, mostrar anuncios invisibles y de fondo y realizar compras no autorizadas en la aplicación utilizando SMS y números de teléfono. Además, el malware Triada tiene la capacidad de robar datos confidenciales, incluidas contraseñas de dispositivos comprometidos.

A. Productos afectados:

- Los investigadores indicaron que el malware Triada afecta dispositivos con sistema operativo Android;
- Los dispositivos afectados incluyen modelos de varias compañías como: Leagoo, ARK Benefit, Zopo Speed, Doogee, Cherry Mobile Flare y muchas otras.

B. Indicadores de compromiso (IoC):

- Sha-256: 748404dd89915e995bdcb8e3fd5589f6edb844868c49550de9f49ef0d641ca71.
- C&C: a3miu[.]h99n6[.]com, ddeur[.]sOve7[.]com, dycsw[.]h99n6[.]com, gjhdr[.]xikuj[.]com, P7819[.]ofqyz[.]com.

3. RECOMENDACIONES:

- Evitar descargar software de fuentes no confiables.
- Descargar siempre aplicaciones de fuentes confiables, ya sean sitios web oficiales o tiendas y repositorios de aplicaciones oficiales.
- Verificar el desarrollador de la aplicación y confirmar la propiedad de la empresa antes de descargar cualquier aplicación. Este enfoque cauteloso puede ayudar a mitigar el riesgo de infecciones de malware y proteger los datos confidenciales.
- Tener cuidado con los permisos solicitados por la aplicación instalada y si son realmente necesarios para la funcionalidad real de la aplicación.

Fuente de Información:	• hxxps://www.hackread.com/triada-malware-android-fake-telegram-app • hxxps://blog.checkpoint.com/security/dont-be-fooled-by-app-earances-check-point-researchers-spot-hidden-malwares-behind-legitimate-looking-apps/