Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°211**	**Fecha: 07-09-2023**
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Pegasus Spyware Exploit encontrado en iPhones que ejecutan el último iOS		
Tipo de Ataque	Spyware	Abreviatura	Spyware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Apple publica una actualización de seguridad urgente ya que se descubre que el exploit de software espía Pegasus, desarrollado por la firma israelí NSO Group, apunta a iPhones sin ninguna interacción del usuario.

Citizen Lab, compañía que descubrió la vulnerabilidad, dijo que llamó a la cadena de exploits BLASTPASS porque involucraba PassKit, un marco que permite a los desarrolladores incluir Apple Pay en sus aplicaciones. Permite a los atacantes comprometer iPhones que ejecutan la última versión de iOS (16.6) sin ninguna interacción por parte de la víctima.

Pegasus es un potente software espía que se puede utilizar para rastrear la ubicación de una víctima, grabar sus llamadas y mensajes e incluso acceder a su cámara y micrófono.

2. DETALLES:

Apple emitió dos CVE relacionados con esta cadena de exploits (CVE-2023-41064 y CVE-2023-41061).

CVE-2023-41064 es un desbordamiento de búfer que se activa al procesar imágenes creadas con fines malintencionados, mientras que CVE-2023-41061 es un problema de validación que puede explotarse mediante archivos adjuntos maliciosos. Ambos permiten a los actores de amenazas obtener la ejecución de código arbitrario en dispositivos iPhone y iPad sin parches.

El exploit involucra archivos adjuntos PassKit que contienen imágenes maliciosas enviadas desde la cuenta de iMessage de un atacante a la víctima. Cuando la víctima abre el archivo adjunto, se ejecuta el código malicioso y el dispositivo se infecta con el software espía Pegasus.

La lista de dispositivos afectados incluye: iPhone 8 y posterior, iPad Pro (todos los modelos), iPad Air de 3ra generación y posteriores, iPad de 5ta generación y posteriores, y iPad mini de 5ta generación y posteriores, Macs con macOS Ventura, y Apple Watch Serie 4 y posteriores.

Apple abordó las fallas en macOS Ventura 13.5.2, iOS 16.6.1, iPadOS 16.6.1 y watchOS 9.6.2 con lógica y manejo de memoria mejorados. Apple lanzó una actualización de seguridad que soluciona la vulnerabilidad BLASTPASS. La actualización está disponible para todos los iPhone con iOS 16.6 y versiones posteriores.

3. RECOMENDACIONES:

- Activar el modo de bloqueo la cual brinda protecciones de seguridad adicionales, como desactivar los archivos adjuntos de iMessage, las conexiones por cable y la autenticación Face ID con dispositivos desconocidos.
- Mantener su software actualizado, según la última versión disponible que lanzó Apple.
- Descargar aplicaciones únicamente de fuentes confiables.
- Utilizar una contraseña segura y habilite la autenticación de dos factores.
- Tener cuidado con los enlaces en los que hace clic y los archivos que abre.
- Sospechar de cualquier correo electrónico o mensaje que solicite información personal.

Fuente de Información:	• hxxps://www.hackread.com/blastpass-pegasus-spyware-exploit-iphones-ios/ • https://www.bleepingcomputer.com/news/security/apple-zero-click-imessage-exploit-used-to-infect-iphones-with-spyware/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°211	Fecha: 07-09-2023
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en el Kernel de Linux		
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:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo error uno por uno y lectura fuera de límites en el Kernel de Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener acceso a información confidencial, realizar un ataque de denegación de servicio (DoS), ejecutar código arbitrario y comprometer el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-38429 de tipo error uno por uno, existe debido a un error uno por uno dentro de la función ksmbd_smb2_check_message() en fs/ksmbd/connection.c. Un atacante remoto puede provocar un error uno por uno y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-38426 de tipo lectura fuera de límites, existe debido a una condición de límite dentro de la función smb2_find_context_vals(). Un atacante remoto puede enviar datos especialmente diseñados al servidor, desencadenar un error de lectura fuera de límites y leer el contenido de la memoria del sistema o realizar un ataque de DoS.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-38428 de tipo lectura fuera de límites, existe debido a un error uno por uno dentro de la función ksmbd_smb2_check_message() en fs/ksmbd/connection.c. Un atacante remoto puede provocar un error uno por uno y ejecutar código arbitrario en el sistema de destino.

A. Productos afectados:

Linux kernel: antes de 6.3.4.

3. RECOMENDACIÓN:

- Actualizar el paquete afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.4