

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 103			Fecha: 03-05-2023
	Página 8 de 13			
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Apple lanza parches de seguridad para iPhone, iPad y Mac			
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC	
Medios de propagación	Red, Internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intento de intrusión			
Descripción				
<p>1. Resumen:</p> <p>Apple lanzó parches de "seguridad rápida" que corrigen múltiples vulnerabilidades de severidad crítica para iPhone, iPad y Mac. Estas vulnerabilidades se encuentran bajo explotación activa o representan riesgos significativos para sus usuarios.</p> <p>La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS).</p> <p>2. Detalles:</p> <ul style="list-style-type: none"> La vulnerabilidad registrada con el código CVE-2022-41723 de severidad alta, de tipo consumo de recursos no controlado, refiere que Un flujo HTTP/2 creado con fines malintencionados podría causar un consumo excesivo de CPU en el decodificador HPACK, lo suficiente como para causar una denegación de servicio a partir de una pequeña cantidad de solicitudes pequeñas. <p>3. Productos afectados:</p> <ul style="list-style-type: none"> Múltiples versiones de iPhone, iPad y Mac <p>4. Solución:</p> <ul style="list-style-type: none"> Las nuevas respuestas rápidas de seguridad se entregan solo para la última versión de iOS, iPadOS y macOS, a partir de iOS 16.4.1, iPadOS 16.4.1 y macOS 13.3.1; Apple recomienda actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades. 				
Fuentes de información	<ul style="list-style-type: none"> https://support.apple.com/en-us/HT201224 			

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 103			Fecha: 03-05-2023
				Página 9 de 13
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Apple lanzó parches de seguridad rápida que corrigen múltiples vulnerabilidades en varios de sus productos			
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC	
Medios de propagación	Red, Internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intento de intrusión			
Descripción				
<p>1. Resumen:</p> <p>Apple lanzó parches de "seguridad rápida" que corrigen múltiples vulnerabilidades de severidad crítica para dispositivos iPhone, iPad y Mac. Estas vulnerabilidades se encuentran bajo explotación activa y representa un riesgo significativo para sus usuarios. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto a comprometer el equipo afectado.</p> <p>2. Detalles:</p> <ul style="list-style-type: none"> La rápida actualización de seguridad llega para los clientes que ejecutan iOS 16.4.1, iPadOS 16.4.1 y macOS 13.3.1. Una vez instalado, agregará una letra a la versión del software, como iOS 16.4.1 (a), iPadOS 16.4.1 (a) y macOS 13.3.1 (a). Los usuarios que ejecuten versiones anteriores del software de Apple no recibirán la corrección de seguridad rápida. Apple dijo que las correcciones se incluirán en las actualizaciones de software posteriores. Cabe señalar, que, en las últimas semanas, los investigadores han descubierto nuevos exploits desarrollados por los fabricantes de spyware QuaDream y NSO Group destinados a los propietarios de iPhone de todo el mundo. Ambos fabricantes de software espía explotaron vulnerabilidades no reveladas previamente en el software de Apple que permitía a sus clientes gubernamentales robar datos del dispositivo de una víctima de forma silenciosa. <p>3. Productos afectados:</p> <ul style="list-style-type: none"> Múltiples versiones de iPhone, iPad y Mac. <p>4. Solución:</p> <ul style="list-style-type: none"> Las nuevas respuestas rápidas de seguridad se entregan solo para la última versión de iOS, iPadOS y macOS, a partir de iOS 16.4.1, iPadOS 16.4.1 y macOS 13.3.1. Una vez instalado, agregará una letra a la versión del software, como iOS 16.4.1 (a), iPadOS 16.4.1 (a) y macOS 13.3.1 (a). Apple recomienda actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades. 				
Fuentes de información	<ul style="list-style-type: none"> https://www.ibm.com/support/pages/node/6987489 			