

Alerta de seguridad informática	9VSA20-00231-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de mayo de 2020
Última revisión	02 de mayo de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Apple referente a una vulnerabilidad crítica que afecta a sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-9859

CVE-2020-3956

El equipo de seguridad Unc0ver descubrió una falla que permitía realizar jailbreaking (obtener permisos de administrador en el dispositivo afectado, eliminando las restricciones de seguridad) en múltiples productos de la línea de Apple.

La vulnerabilidad en memoria afecta al kernel de los sistemas operativos de Apple y permite que una aplicación especialmente diseñada logre la ejecución de código a nivel de kernel, fuera del entorno de aislamiento de procesos (sandbox). La explotación también funciona en dispositivos modernos que utilicen una CPU que admita PAC (Pointer Authentication Code), por lo que se puede saber que PAC no previene la vulnerabilidad.

Productos Afectados

Apple Watch Series 1 y posteriores.

Apple TV 4K y Apple TV HD.

macOS High Sierra 10.13.16.

macOS Catalina 10.15.5.

iPhone 6s y posteriores.

iPad Air 2 y posteriores.

iPad Mini 4 y posteriores.

iPod Touch 7th generation.

Mitigación

Para Apple Watch Series 1 y posteriores, actualizar a la versión 6.2.6 de watchOS.

Para Apple TV 4K y Apple TV HD, actualizar a la versión 13.4.6 de tvOS.

Para macOS High Sierra 10.13.6 aplicar actualización de seguridad 2020-003.

Para macOS Catalina 10.15.5 aplicar actualización suplemental 10.15.5.

Para iPhone 6s y posteriores, iPad Air 2 y posteriores, iPad mini 4 y posteriores, e iPod touch 7th generation, actualizar a la versión iOS 13.5.1 o iPadOS 13.5.1.

Enlaces

<https://support.apple.com/en-us/HT201222>

<https://support.apple.com/en-us/HT211217>

<https://support.apple.com/en-us/HT211216>

<https://support.apple.com/en-us/HT211215>

<https://support.apple.com/en-us/HT211214>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3956>