Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Apple Lanzó actualizaciones de seguridad, para corregir dos Zero Day en sus dispositivos.

19/Agosto/2022

Contenido

INTRODUCCIÓN

Apple lanza dos actualizaciones de emergencia para corregir vulnerabilidades de día cero en sus dispositivos, si usted es poseedor de dispositivos Apple considere actualizar a la brevedad.

VULNERABILIDADES DE DÍA CERO CORREGIDAS POR APPLE.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_08_19_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/12/2022
Es día cero (0 day):	SI (CVE-2022-32894 and CVE-2022-32893)

RESUMEN

Apple lanzó actualizaciones de seguridad de emergencia para corregir dos vulnerabilidades de día cero que los atacantes explotaron anteriormente para piratear iPhones, iPads o Macs.

Las vulnerabilidades de día cero son fallas de seguridad conocidas por atacantes o investigadores antes de que el proveedor de software se dé cuenta o pueda repararlas. En muchos casos, los días cero tienen exploits de prueba de concepto públicos o se explotan activamente en ataques.

Apple ha lanzado macOS Monterey 12.5.1 e iOS 15.6.1/iPadOS 15.6.1 para resolver dos vulnerabilidades de día cero que, según se informa, han sido explotadas activamente.

Las dos vulnerabilidades son las mismas para los tres sistemas operativos, siendo la primera rastreada como CVE-2022-32894. Esta vulnerabilidad es una vulnerabilidad de escritura fuera de los límites en el Kernel del sistema operativo.

El kernel es un programa que funciona como el componente central de un sistema operativo y tiene los privilegios más altos en macOS, iPadOS e iOS.

Una aplicación, como un malware, puede usar esta vulnerabilidad para ejecutar código con privilegios de Kernel. Como este es el nivel de privilegio más alto, un proceso podría realizar cualquier comando en el dispositivo, tomando efectivamente el control completo sobre él.

La segunda vulnerabilidad de día cero es CVE-2022-32893 y es una vulnerabilidad de escritura fuera de los límites en WebKit, el motor de navegador web utilizado por Safari y otras aplicaciones que pueden acceder a la web.

Apple dice que esta falla permitiría a un atacante realizar la ejecución de código arbitrario y, como está en el motor web, probablemente podría explotarse de forma remota al visitar un sitio web creado con fines malintencionados.

Los errores fueron informados por investigadores anónimos y Apple los corrigió en iOS 15.6.1, iPadOS 15.6.1 y macOS Monterey 12.5.1 con una verificación de límites mejorada para ambos errores.

La lista de dispositivos afectados por ambas vulnerabilidades es:

- Mac con macOS Monterey
- iPhone 6s y posteriores
- iPad Pro (todos los modelos), iPad Air 2 y posteriores, iPad de 5.ª generación y posteriores, iPad mini 4 y posteriores y iPod touch (7.ª generación).

Apple reveló la explotación activa en la naturaleza, sin embargo, no publicó ninguna información adicional sobre estos ataques.

Probablemente, estos días cero solo se usaron en ataques dirigidos, pero aun así se recomienda encarecidamente instalar las actualizaciones de seguridad de hoy lo antes posible.

Siete días cero parcheados por Apple este año

En marzo, Apple corrigió otros dos errores de día cero que se usaron en el controlador de gráficos Intel (CVE-2022-22674) y AppleAVD (CVE-2022-22675) que también podrían usarse para ejecutar código con privilegios de kernel.

En enero, Apple parcheó dos días cero más explotados activamente que permitieron a los atacantes lograr la ejecución de código arbitrario con privilegios de kernel (CVE-2022-22587) y rastrear la actividad de navegación web y las identidades de los usuarios en tiempo real (CVE-2022-22594).

En febrero, Apple lanzó actualizaciones de seguridad para corregir un nuevo error de día cero explotado para piratear iPhones, iPads y Mac, lo que provocó fallas en el sistema operativo y ejecución remota de código en dispositivos comprometidos después de procesar contenido web creado con fines malintencionados.

RECOMENDACIONES

- Verificar si sus dispositivos Apple son afectados y proceder a la actualización de sistema.
- Si su dispositivo presenta funcionamiento anormal, antes de realizar la actualización aplicar un factory reset.
- No permita que Safari recuerde sus credenciales, los dispositivos Apple tienen su bóveda de contraseñas dentro de los ajustes en la sección de contraseñas.

Noticia Completa

https://devel.group/actualizaciones-de-seguridad-de-apple-corrigen-2-dias-cero-utilizados-para-hackear-iphones-macs/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente