Alerta de seguridad cibernética	9VSA23-00811-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de dos vulnerabilidades de día cero parchadas por Apple en sus actualizaciones iOS 16.4.1, iPadOS 16.4.1.

Vulnerabilidades

CVE-2023-28206 CVE-2023-28205

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-28206: Una app puede ejecutar código arbitrario con privilegios del kernek. Apple señaló que tiene conocimiento de un reporte que indica que este problema puede haber sido activamente explotado.

CVE-2023-28205: Procesar contenido web malicioso puede llevar a ejecución arbitraria de código. Apple señaló que tiene conocimiento de un reporte que indica que este problema puede haber sido activamente explotado.

Productos afectados

iPhone 8 y posterior, iPad Pro (todos), iPad Air 3ra generación y posteriores, iPad 5ta generación y posteriores, iPad mini 5ta generación y posteriores.

Enlaces

https://support.apple.com/es-cl/HT213720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28206
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28205

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.10 10:51:34 -04'00'