

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	9VSA24-00961-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2024
Última revisión	23 de enero de 2024

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 vulnerabilidades parchadas por Apple en su más reciente versión de los sistemas operativos para sus iPhones y iPads, iOS 17.3 y iPadOS 17.3.

Vulnerabilidades

[CVE-2024-23212](#)

[CVE-2024-23218](#)

[CVE-2024-23208](#)

[CVE-2024-23207](#)

[CVE-2024-23223](#)

[CVE-2024-23219](#)

[CVE-2024-23211](#)

[CVE-2024-23203](#)

[CVE-2024-23204](#)

[CVE-2024-23217](#)

[CVE-2024-23210](#)

[CVE-2024-23206](#)

[CVE-2024-23213](#)

[CVE-2024-23214](#)

[CVE-2024-23222](#)

[CVE-2024-23215](#)

[CVE-2023-42916](#)

[CVE-2023-42917](#)

Impacto

Vulnerabilidades de riesgo crítico:

Apple no indicó el nivel de severidad de las vulnerabilidades.

Mitigación

Actualizar los dispositivos compatibles, a iOS 17.3 y iPadOS 17.3.

Productos afectados

iPhone XS y posteriores, iPad Pro 12.9-inch 3ra generación y posteriores, iPad Pro 11-inch 1ra generación y posteriores, iPad Air 3ra generación y posteriores, iPad 8va generación y posteriores, y iPad mini 5ta generación y posteriores.

Enlaces

<https://support.apple.com/en-us/HT214059>

<https://support.apple.com/en-us/HT214062>