

Alerta de seguridad cibernética	9VSA21-00512-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2021
Última revisión	27 de octubre de 2021

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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades en productos de Apple.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-30821	CVE-2021-30888	CVE-2021-30910
CVE-2021-30824	CVE-2021-30899	CVE-2021-30911
CVE-2021-30834	CVE-2021-30900	CVE-2021-30912
CVE-2021-30868	CVE-2021-30901	CVE-2021-30913
CVE-2021-30876	CVE-2021-30902	CVE-2021-30915
CVE-2021-30877	CVE-2021-30903	CVE-2021-30916
CVE-2021-30879	CVE-2021-30906	CVE-2021-30917
CVE-2021-30880	CVE-2021-30907	CVE-2021-30918
CVE-2021-30881	CVE-2021-30908	CVE-2021-30919
CVE-2021-30883	CVE-2021-30909	

Impactos

Riesgo alto:

CVE-2021-30881: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema, debido a una validación insuficiente de los inputs del usuario en FileProvider.

CVE-2021-30883: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema, debido a un error de límites de memoria dentro del subsistema IOMobileFrameBuffer.

Esta vulnerabilidad ya estaría siendo explotada.

CVE-2021-30917: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema, debido a un error de límites de memoria al procesar perfiles ICC en el subsistema ColorSync.

CVE-2021-30919: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema, debido a un error de límites de memoria dentro del subsistema CoreGraphics al procesar archivos PDF.

Productos Afectados

MacOS 11.0 20A2411 a 11.6 20G165.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<http://support.apple.com/en-us/HT212868>

<http://support.apple.com/en-us/HT212872>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30821>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30824>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30834>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30868>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30876>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30877>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30879>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30880>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30881>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30883>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30888>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30899>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30900>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30901>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30902>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30903>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30906>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30907>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30908>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30909>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30910>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30911>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30912>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30913>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30915>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30916>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30917>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30918>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30919>