Alerta de seguridad cibernética	9VSA22-00562-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2022
Última revisión	27 de enero de 2022

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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre múltiples vulnerabilidades en Apple watchOS.

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

Vulnerabilidades

CVE-2022-22584
CVE-2022-22578
CVE-2022-22585
CVE-2022-22593
CVE-2022-22590
CVE-2022-22592
CVE-2022-22589
CVE-2022-22594

Impactos

Vulnerabilidad de riesgo alto

CVE-2022-22584: Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra, provocar daños en la memoria y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.

CVE-2022-22578: La vulnerabilidad permite que una aplicación maliciosa aumente los privilegios en el sistema.

CVE-2022-22585: La vulnerabilidad permite que una aplicación maliciosa obtenga acceso a información confidencial.

CVE-2022-22593: Un usuario local o una aplicación malintencionada puede desencadenar un desbordamiento del búfer y ejecutar código arbitrario con privilegios de kernel.

CVE-2022-22590: Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada, desencadenar un error de uso después de liberar y ejecutar código arbitrario en el sistema. La explotación exitosa de la vulnerabilidad puede permitir que un atacante comprometa un sistema vulnerable.

CVE-2022-22592: Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y evitar que se aplique la política de seguridad de contenido.

CVE-2022-22589: La vulnerabilidad permite que un atacante remoto ejecute código JavaScript arbitrario en el sistema.

CVE-2022-22594: La vulnerabilidad permite que un atacante remoto obtenga acceso a información potencialmente confidencial.

Productos afectados

Sistema operativo del reloj: 8.0 19R346, 8.1 19R570, 8.1.1 19R580, 8.3 19S55

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.apple.com/en-us/HT213059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22584
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22593

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22590
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22589
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22594

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.27 08:49:00 -03'00'