Alerta de seguridad cibernética	9VSA20-00164-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2020
Última revisión	30 de marzo de 2020

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, CSIRT, comparte la información entregada por Apple referente a diversas vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

VULNERABILIDADES

CVE-2020-3883
CVE-2020-3885
CVE-2020-3887
CVE-2020-3888
CVE-2020-3890
CVE-2020-3891
CVE-2020-3894
CVE-2020-3895
CVE-2020-3897
CVE-2020-3899
CVE-2020-3900
CVE-2020-3901
CVE-2020-3902
CVE-2020-3909
CVE-2020-3910
CVE-2020-3913
CVE-2020-3914
CVE-2020-3916
CVE-2020-3919
CVE-2020-9768
CVE-2020-9770
CVE-2020-9773
CVE-2020-9775
CVE-2020-9777
CVE-2020-9780
CVE-2020-9781
CVE-2020-9783
CVE-2020-9784
CVE-2020-9785

Vulnerabilidades Apple

Impacto

Apple ha lanzado parches de seguridad para subsanar múltiples vulnerabilidades en sus productos, una de ellas, para macOS, permitía a un atacante en posición de red privilegiada interceptar tráfico bluetooth, lo cual afecta a la privacidad de las personas, también había una falla en el correo que permitía a un usuario local ver contenido eliminado en el selector de las aplicaciones. En safari se encontró una vulnerabilidad que permitía obtener permisos del usuario sin que estos se enteraran. Entre los elementos que más vulnerabilidades tuvieron en esta actualización de seguridad fueron el WebKit, presentando errores que permitían ataques cross-site scripting, ejecución de código arbitrario entre otras fallas, y también los errores en Kernel, permitiendo a atacantes comprometer al sistema.

Productos Afectados

Se han visto afectados los productos iOS, watchOS, iPadOS y Safari.

Mitigación

Se deben aplicar los parches desarrollados por Apple.
Para iOS aplicar versión 13.4.
Para iPadOS aplicar versión 13.4.
Para watchOS aplicar versión 6.2.
Para Safari aplicar versión 13.1.

Enlaces

iOS e iPadOS:
https://support.apple.com/en-hk/HT211102

watchOS:
https://support.apple.com/en-il/HT211103
https://seclists.org/fulldisclosure/2020/Mar/33

Safari:
https://support.apple.com/en-eg/HT211104
https://seclists.org/fulldisclosure/2020/Mar/35

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.30 20:15:04 -03'00'