Alerta de seguridad informática	9VSA-00074-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de octubre de 2019
Última revisión	30 de octubre de 2019

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 correspondiente a múltiples vulnerabilidades en watchOS, Safari, iOS, iPadOS, macOS Catalina y tvOS.

Vulnerabilidad

CVE-2017-7152
CVE-2018-12152
CVE-2018-12153
CVE-2018-12154
CVE-2019-8509
CVE-2019-8706
CVE-2019-8708
CVE-2019-8715
CVE-2019-8716
CVE-2019-8736
CVE-2019-8737
CVE-2019-8743
CVE-2019-8744
CVE-2019-8747
CVE-2019-8749
CVE-2019-8750
CVE-2019-8756
CVE-2019-8759
CVE-2019-8761
CVE-2019-8764
CVE-2019-8765
CVE-2019-8766
CVE-2019-8767
CVE-2019-8775
CVE-2019-8782
CVE-2019-8783
CVE-2019-8784
CVE-2019-8785
CVE-2019-8786
CVE-2019-8787
CVE-2019-8788
CVE-2019-8789
CVE-2019-8793
CVE-2019-8794
CVE-2019-8795
CVE-2019-8797
CVE-2019-8798
CVE-2019-8801
CVE-2019-8802
CVE-2019-8803
CVE-2019-8804
CVE-2019-8805
CVE-2019-8807
CVE-2019-8808
CVE-2019-8811
CVE-2019-8812
CVE-2019-8813
CVE-2019-8814
CVE-2019-8815
CVE-2019-8816
CVE-2019-8817
CVE-2019-8819
CVE-2019-8820
CVE-2019-8821
CVE-2019-8822
CVE-2019-8823

Impacto

Se han descubierto múltiples vulnerabilidades en watchOS, Safari, iOS, iPadOS, macOS Catalina y tvOS. La más grave de estas vulnerabilidades podría permitir la ejecución de código arbitrario. Los detalles de estas vulnerabilidades son los siguientes:

- Existía un problema de coherencia al decidir cuándo mostrar el indicador de grabación de pantalla. El problema se resolvió con una mejor gestión del estado. (CVE-2019-8793)
- Se solucionó un problema de denegación de servicio con una validación mejorada. (CVE-2019-8737)
- Existía un problema de carga dinámica de la biblioteca en la configuración de iTunes. Esto se solucionó con una mejor búsqueda de ruta. (CVE-2019-8801)
- Se solucionó un problema lógico con restricciones mejoradas. (CVE-2019-8708)
- Se solucionó un problema de consumo de memoria mejorando el manejo de la memoria. (CVE-2019-8767)
- Existía un problema de corrupción de memoria en el manejo de paquetes IPv6. Este problema se solucionó mejorando la administración de la memoria. (CVE-2019-8744)
- Se solucionó un problema de corrupción de memoria mejorando la administración del estado. (CVE-2019-8706)
- Se corrigió una vulnerabilidad de corrupción de memoria con un bloqueo mejorado. (CVE-2019-8747)
- Se solucionó un problema de autenticación con una gestión de estado mejorada. (CVE-2019-8803)
- Se solucionó una inconsistencia en la configuración de la red Wi-Fi. (CVE-2019-8804)
- Se solucionó un problema de interfaz de usuario incoherente con una gestión de estado mejorada. (CVE-2017-7152)
- Se solucionó un problema de validación de entrada mejorando la validación de entrada. (CVE-2019-8736)
- Existía un problema en el análisis de las URL. Este problema se solucionó con una validación de entrada mejorada. (CVE-2019-8788)
- Una lectura fuera de límites se abordó con una mejor verificación de límites. (CVE-2019-8759)
- Una lectura fuera de límites se abordó con una validación de entrada mejorada. (CVE-2019-8787)
- Existía un problema de validación en la verificación de derechos. Este problema se solucionó con una validación mejorada de los derechos del proceso. (CVE-2019-8805)
- Existía un problema de validación en el manejo de enlaces simbólicos. Este problema se solucionó con una validación mejorada de los enlaces simbólicos. (CVE-2019-8789)
- Se solucionó un problema de validación con una lógica mejorada. (CVE-2019-8802)
- Se abordaron múltiples problemas de lógica mejorando la gestión del estado. (CVE-2019-8764, CVE-2019-8813)
- Se abordaron múltiples problemas de corrupción de memoria con una validación de entrada mejorada. (CVE-2018-12152, CVE-2018-12153, CVE-2018-12154, CVE-2019-8749, CVE-2019-8750, CVE-2019-8756)

- Se abordaron múltiples problemas de corrupción de memoria mejorando el manejo de la memoria. (CVE-2019-8715, CVE-2019-8716, CVE-2019-8784, CVE-2019-8785, CVE-2019-8786, CVE-2019-8795, CVE-2019-8797, CVE-2019-8798, CVE -2019-8807)
- Se abordaron múltiples problemas de corrupción de memoria mejorando el manejo de la memoria. (CVE-2019-8743, CVE-2019-8765, CVE-2019-8766, CVE-2019-8782, CVE-2019-8783, CVE-2019-8808, CVE-2019-8811, CVE-2019-8812, CVE -2019-8814, CVE-2019-8815, CVE-2019-8816, CVE-2019-8819, CVE-2019-8820, CVE-2019-8821, CVE-2019-8822, CVE-2019-8823)
- Se abordaron múltiples problemas de validación mejorando la desinfección de insumos. (CVE-2019-8794, CVE-2019-8817)
- El problema se solucionó restringiendo las opciones ofrecidas en un dispositivo bloqueado. (CVE-2019-8775)
- Este problema se solucionó eliminando el código vulnerable. (CVE-2019-8509)
- Este problema se solucionó con controles mejorados. (CVE-2019-8761)

Productos Afectados

- iOS versiones anteriores a 13.2
- iPadOS versiones anteriores a 13.2
- Safari versiones anteriores a 13.0.3
- watchOS versiones anteriores a 6.1
- macOS Catalina versiones anteriores a 10.15.1
- tvOS versiones anteriores a 13.2

Mitigación

Aplicar las actualizaciones a las versiones publicadas por el fabricante según corresponda.

Enlace

https://support.apple.com/en-us/HT210721
https://support.apple.com/en-us/HT210722
https://support.apple.com/en-us/HT210723
https://support.apple.com/en-us/HT210724
https://support.apple.com/en-us/HT210725
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2019-117/

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.30 17:04:26 -03'00'