Nro. Alerta:	EC-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**ACTUALIZACIÓN DE SEGURIDAD PRODUCTOS APPLE**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades
Tipo de incidente: Acceso no autorizado a espacios de memoria
Nivel de riesgo: Medio

II. ALERTA

Apple emite actualizaciones de seguridad para corregir vulnerabilidades encontradas en varios tipos de productos. Las actualizaciones gestionan ciertas vulnerabilidades de tipo Zero Day

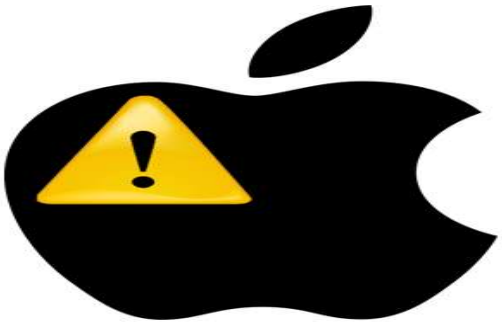

Figura 1.- Alerta Vulnerabilidades Apple
Fuente: EcuCERT

III. INTRODUCCIÓN

Durante el año 2022 se han emitido reportes de vulnerabilidades de seguridad relacionados con productos APPLE, quien a su vez ha emitido varias actualizaciones de seguridad a fin de mitigar los riesgos asociados a las vulnerabilidades detectadas. En los reportes de seguridad se han señalado vulnerabilidad de tipo Zero-Day, las cuales representan para los actores maliciosos una oportunidad de ataque sin defensa. En análisis de priorización de gestión de riesgo relacionado a las vulnerabilidades detectadas se encuentran en CVE-2022-22587, CVE-2022-22594, CVE-2022-22620, CVE-2022-22674 y CVE-2022-22675

Las técnicas de explotación de las vulnerabilidades reportadas incluyen la exhalación de privilegios, inyección de código y ejecución de código por parte del usuario.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**ACTUALIZACIÓN DE SEGURIDAD PRODUCTOS APPLE**	V 1.1

Los productos afectados incluyen a los siguientes

- Navegador Safari, versiones anteriores a 15.5
- Sistema operativo tvOS, versiones anteriores a 15.5
- Xcode, versiones anteriores a 13.4
- Sistema operativo macOS Catalina, actualización de seguridad anterior a Security Update 2022-004
- Sistema operativo macOS Big Sur, versiones anteriores a 11.6
- Sistema operativo macOS Monterey, versiones anteriores a 12.4
- iOS y iPadOS versiones anteriores a 15.5
- watchOS versiones anteriores a 8.6

De acuerdo a las notificaciones de seguridad emitidas por el fabricante, se ha detectado la activa explotación de las vulnerabilidades reportadas, por lo cual se hace prioritario ejecutar las acciones de mitigación, enfocadas en garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

IV. VECTOR DE ATAQUE:

La explotación de las vulnerabilidades reportadas inicia con la descarga de paquetes maliciosos, que suelen visualizarse como aplicaciones validas, y la redirección hacia sitios web maliciosos en los que automáticamente se ejecuta la descarga de archivos maliciosos.

V. IMPACTO:

Al explotar las vulnerabilidades reportadas un atacante podría lograr que el sistema vulnerable ejecute código malicioso con privilegios de gestión a nivel de Kernel, así como también se acceda a espacios de memoria no autorizados.

VI. INDICADORES DE COMPROMISO:

Al momento el fabricante no ha hecho público indicadores de compromiso específicos relacionados a las técnicas y herramientas de explotación de las vulnerabilidades reportadas.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**ACTUALIZACIÓN DE SEGURIDAD PRODUCTOS APPLE**	V 1.1

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar el sistema operativo de productos Apple de acuerdo a lo indicado por el fabricante.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida e indisponibilidad de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Tener actualizado y utilizar, un software anti-virus

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- Apple. (16 de 05 de 2022). *Apple*. Obtenido de Apple: https://support.apple.com/es-es/HT201222.
- nakedsecurity. (17 de 05 de 2022). *nakedsecurity*. Obtenido de nakedecurity: https://nakedsecurity.sophos.com/2022/05/17/apple-patches-zero-day-kernel-hole-and-much-more-update-now/
- Threatpost. (11 de 02 de 2022). *Threatpost*. Obtenido de Threatpost: https://threatpost.com/apple-patches-actively-exploited-webkit-zero-day/178370//www.2-spyware.com/remove-quantum-locker-ransomware.html

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec