
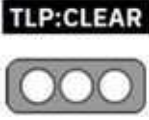


Nro. Alerta:	AL-2023-44	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	29/09/2023	Parches de Seguridad de Apple.	Pág.:1of3

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: **Alto**


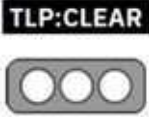
II. ALERTA

Apple generaría diferentes tipos de parches de seguridad los cuales cubrirían tres fallas, las cuales se han venido explotando en últimamente ya que estaría afectando a las actividades de los diferentes dispositivos los cuales son iOS, iPadOS, macOS y Safari.



Figura 1.-Ilustración relacionada a Apple
 Fuente: <https://cultura-informatica.com/apple/apple-lanza-parche-ios-ipados-y-macos/>



Nro. Alerta:	AL-2023-	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	25/09/2023	Parches de Seguridad en Apple.	Pág.:2of3

III. INTRODUCCIÓN

Las actividades que Apple realizado en mejorar sus sistemas de seguridad han sido grandes ya que este último año se a encontrado alrededor de 16 fallas de seguridad las cuales se corrigieron con el tiempo, algunas de las vulnerabilidades que se estaban presentando son las:

- **CVE-2023-41991**.- La cual presentaba un sistema de validación en cuanto a los certificados en el marco de la seguridad y esto permitiría que una de aplicación maliciosa omita la validación de firmas.
- **CVE-2023-41992**.- Esta tendría fallas en el Kernel lo que permitiría que un atacante local se permita escalar diferentes privilegios.
- **CVE-2023-41993**.-Esto lo que aria es generar una falla en el WebKit lo que provocaría que pueda ejecutar código malicioso de manera arbitraria al procesar diferente contenido a la web diseñado especialmente.

En este punto lo que Apple pregona que las falla ya han sido contenida ya que con la generación de nuevos parches de seguridad estarían cubriendo el déficit que se mantenía en los modelos posteriores al iOS 16.7.

Las personas a las que se les atribuye el haber detectado estas fallas de seguridad son a personas de la Universidad de Toronto.

La divulgación de estas fallas de vulnerabilidades se presenta con una diferencia de dos días a que Apple habría resuelto otras dos fallas de seguridad las cuales estaban encadenadas y de esta manera tener una cadena de exploits de mensajería el cual estaba denominado como BLASTPASS el cual estar implementado un software de espionaje mercenario.

Conjuntamente con esto de le fueron sumando diferentes errores los cuales está relacionado a las imágenes, pero por otro lado está ya quedaría solucionado con el ultimo parche de seguridad.

IV. VECTOR DE ATAQUE:

- Instalación y ejecución de software malicioso.



<https://www.ecucert.gob.ec>



@EcuCERT_EC


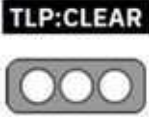
Agencia de Regulación y Control de las Telecomunicaciones

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:	AL-2023-	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	25/09/2023	Parches de Seguridad en Apple.	Pág.:3of3

V. IMPACTO:

- Escalabilidad de privilegios.
- Instalación no autorizada de aplicaciones.
- Procesamiento de imágenes especialmente diseñadas.

VI. RECOMENDACIONES:

- Mantener actualizados los diferentes parches de seguridad del sistema operativo.
- Revisar el listado de productos los cuales todavía cuentan con el soporte de la marca y las debidas actualizaciones.
- Aplicar el principio de menor privilegio en la creación de perfiles de usuario.

VII. REFERENCIAS:

- NIST. CVE-2023-41991. (21 de 09 de 2023). Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2023-41991>
- NIST. CVE-2023-41992. (25 de 09 de 2023). Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2023-41992>
- NIST. CVE-2023-41993. (25 de 09 de 2023). Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2023-41993>



<https://www.ecucert.gob.ec>



@EcuCERT_EC

Agencia de Regulación y Control de las Telecomunicaciones

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel

Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

www.arcotel.gob.ec