Nro. Alerta:	EC-2022-63	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-abril-2022	**Vulnerabilidad en 7-ZIP**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades
Tipo de incidente: Sistema o Software Abierto
Nivel de riesgo: Medio

II. ALERTA

El compresor de archivos gratuito y de código libre “7-ZIP” presenta una vulnerabilidad que permitiría a un atacante remoto escalamiento de privilegios y ejecución de comandos.

Figura 1. Ilustración relacionada a 7-ZIP
Fuente: 7-Zip.org

III. INTRODUCCIÓN

Este software gratuito y de código abierto que permite la compresión y descompresión de archivos en diferentes formatos como: 7z, XZ, BZIP2, GZIP, TAR, ZIP, WIM, ARJ, CAB, ISO, RAR, Z, entre otros.

Entre las características de 7-Zip, se mencionan:

- Para los formatos ZIP y GZIP, 7-Zip proporciona una relación de compresión que es 2-10 % mejor que la relación proporcionada por PKZip y WinZip.
- Fuerte cifrado AES-256 en formatos 7z y ZIP.
- Capacidad de auto extracción para formato 7z.
- Integración con Windows Shell.
- Potente administrador de archivos.
- Potente versión de línea de comandos.
- Complemento para FAR Manager.
- Localizaciones para 87 idiomas.

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-2022-63	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-abril-2022	**Vulnerabilidad en 7-ZIP**	Versión 1.0

En este sentido, la vulnerabilidad identificada como **CVE-2022-29072** permitiría a un atacante realizar el escalamiento de privilegios y la ejecución de comandos; siendo las versiones afectadas hasta la "7-Zip 21.07".

Figura 1. Versión afectada por CVE-2022-29072
Fuente: 7-zip

IV. **VECTOR DE ATAQUE:** Remoto

Esta vulnerabilidad se presenta; debido a una incorrecta configuración de la librería "7z.dll" y un desbordamiento de montón (heap overflow) ocasionada por una inyección de comandos del ejecutable "hh.exe"; provocando que un atacante pueda realizar un escalamiento de privilegios; esto ocurre cuando se arrastra un archivo con la extensión ".7z" al área Ayuda y posteriormente la sección contenido como se indica en la siguiente figura.

Nro. Alerta:	EC-2022-63	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-abril-2022	**Vulnerabilidad en 7-ZIP**	Versión 1.0

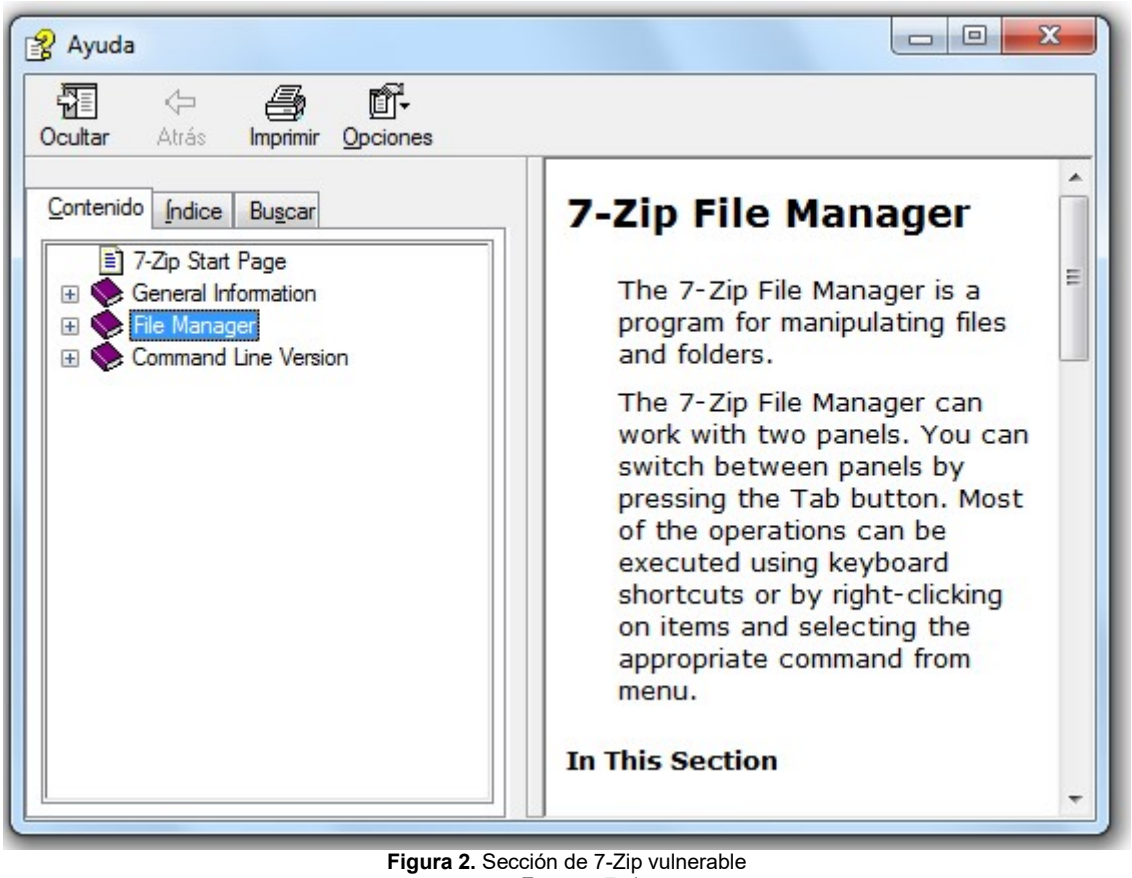

Figura 2. Sección de 7-Zip vulnerable
Fuente: 7-zip

V. IMPACTO:

CVE-2022-29072 posee una CVSS temporal de 6.1 y las versiones afectadas de 7-ZIP en Windows corresponden hasta la 21.07. Como se mencionó anteriormente, el componente "Extension" es afectada por esta vulnerabilidad y mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios y ejecución de comandos; teniendo repercusión sobre la confidencialidad, integridad y disponibilidad.

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

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- En el caso de que no esté disponible una actualización, se sugiere que el programa 7-zip solo tenga asignado permisos de lectura y ejecución para todos los usuarios.
- Si el fabricante no ha emitido las contramedidas necesarias, se sugiere sustituir el producto por un equivalente.

VII. REFERENCIAS:

7ZIP. (s.f.). *7-ZIP*. Obtenido de 7-ZIP: https://www.7-zip.org/

NIST, N. (19 de 04 de 2022). *NVD NIST*. Obtenido de NVD NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-29072

PARAGUAY, C. (19 de 04 de 2022). *CERT GOB PY*. Obtenido de CERT GOB PY: https://www.cert.gov.py/application/files/2616/5039/5065/BOL-CERT-PY-2022-21_Vulnerabilidad_de_escalamiento_de_privilegios_en_7-zip_.pdf

Soto, J. (s.f.). *Geeknetic*. Obtenido de Geeknetic: https://www.geeknetic.es/7-Zip/que-es-y-para-que-sirve#:~:text=7%2Dzip%20sirve%20para%20comprimir,o%20varios%20si%20queremos%20partirlo

VulDB. (16 de 04 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.197545