BOLETÍN DE ALERTA

Boletín Nro.: 2022-21

Fecha de publicación: 19/04/2022

Fecha de actualización: 22/04/2022

Tema: Vulnerabilidad de escalamiento de privilegios en 7-zip

Versiones afectadas:

- 7-Zip hasta la versión 21.07 en la plataforma Windows.

Descripción:

Se ha detectado una vulnerabilidad en 7-zip, que permitiría a un atacante remoto realizar escalamiento de privilegios y ejecución de comandos.

La vulnerabilidad identificada como CVE-2022-29072, sin severidad asignada aún. Esta falla se debe a una incorrecta configuración de la librería "7z.dll" y un desbordamiento de montículo (*heap overflow*) ocasionada por una inyección de comandos del ejecutable "hh.exe", que permitiría a un atacante realizar escalamiento de privilegios administrativos y ejecución de comandos cuando se arrastra un archivo con la extensión ".7z" al área Help>Contents del software 7-zip.

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante realizar escalamiento de privilegios administrativos y ejecución de comandos.

Detección:

Verificar si se posee instalado la versión afectada en el equipo.

- 7-Zip hasta la versión 21.07 en la plataforma Windows.

Mitigación:

Actualmente, no se cuenta con una solución oficial, sin embargo, se recomienda seguir los siguientes pasos para obtener posibles soluciones:

1. Si 7-zip no se actualiza, eliminar el archivo 7-zip.chm será suficiente para mitigar la vulnerabilidad.

2. El programa 7-zip solo debe tener asignado permisos de lectura y ejecución (para todos los usuarios).

Adicionalmente, se sugiere para detección y mitigación la herramienta proporcionada en el siguiente enlace:

- https://github.com/tiktb8/CVE-2022-29072

ACTUALIZACIÓN IMPORTANTE:

La vulnerabilidad **7zip** CVE-2022-29072 se ha marcado como "disputada" (o en disputa) en la lista oficial, además "existen múltiples reportes de investigadores informando que no han podido reproducir una escalada de privilegios" como se anunció inicialmente.

Según el investigador de vulnerabilidades de Google Project Zero, Tavis Ormandy, quien habría alertado sobre la disputa, este exploit solo podría ocurrir al editar el registro y posiblemente otras maniobras (como agregar otra cuenta de administrador local). Sin embargo, la descripción proveída por el que reporto la vulnerabilidad no es lo suficientemente clara para discernir el método de ataque.

Desde el CERT-PY mantendremos informando al respecto sobre novedades en el incidente.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2022-29072
- https://github.com/kagancapar/CVE-2022-29072
- https://twitter.com/MeAsHacker_HNA/status/1515533146636312587
- https://www.cve.org/CVERecord?id=CVE-2022-29072
- https://www.tomshardware.com/news/7-zip-zero-day-exploit