Hive Pro

THREAT ADVISORY

What will be the consequence of this disputed vulnerability in 7-ZIP?

TA2022100

Threat Level RED

Publish Date – April 26, 2022

The zero-day vulnerability in 7- Zip software, tracked as CVE-2022-29072 is marked as disputed by the National Vulnerability Database(NVD), and sparked discussions over its consequences. This started when a researcher published a proof-of-concept (POC) for this vulnerability and stated that it allowed remote privilege escalation. However, other well-known researchers, such as those from Google's Project Zero, have indicated that this security flaw would allow execution of arbitrary code via 7-Zip while opening a file with the.7z extension.

The impact of this vulnerability remains uncertain and due to non availability of patch and a proof-of-concept been widely available, Hive pro Threat research team recommends to temporarily resolve this issue by deleting the Help file. The following are the steps to do this:

1. Open the 7-Zip installation directory or folder on the system
2. Locate the file 7-Zip.chm; this is the help file
3. Right-click on the file and select the Delete context menu option, to remove it from the system.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.005: Obtain Capabilities: Exploits
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-29072	7-Zip versions 2.00 to 21.07	cpe:2.3:a:7-zip_org:7-zip:*:*:*:*:*:*:*:*	A vulnerability in 7-zip on Windows OS	CWE-122

References

https://github.com/kagancapar/CVE-2022-29072
https://www.geektopia.es/es/technology/2022/04/20/noticias/un-fallo-de-seguridad-en-7-zip-es-menos-grave-de-lo-inicialmente-indicado.html