WinRAR patch is issued but the unpatched are at risk

19 March 2019, by Nancy Cohen

Credit: CC0 Public Domain

OK, this bug was nasty.

WinRAR was discovered to have a critical vulnerability. Eric Hamilton in *TechSpot*: malicious archive files were "booby trapped," he said.

Long and short, Rarlab issued a patch. But wait a minute. Hamilton said that "hackers are leveraging the exploit to reach vulnerable systems before users update," and "those who are not using the most recent version are still at risk."

(McAfee advised users to keep their anti-malware signatures up to date at all times.)

"WinRAR—What's new in the latest version, Version 5.70" can be checked out on the WinRAR site.

What is WinRAR? It can back up your data. It can reduce the size of email attachments. It can decompress ZIP and other files downloaded from the Internet and create new archives in RAR and ZIP file format.

It has about 500 million users. Hamilton said, "most of which probably don't know about this vulnerability and that creates a desirable attack surface."

At this point, it would be helpful for computer users to check out the McAfee site for Craig Schmugar's blog about the vulnerability. "While a patched version, 5.70, was released on February 26, attackers are releasing exploits in an effort to reach vulnerable systems before they can be patched."

Schugar said the user is totally blind to the possibility that a malicious payload had perhaps been created in the Startup folder behind the scenes. As no alert is displayed to the user, at the next time the system restarts, the malware is run.

"The absolute path traversal made it possible for archive files to extract to the Windows startup folder (or any other folder of the archive creator's choosing) without generating a warning," said Dan Goodin in *Ars Technica*. "From there, malicious payloads would automatically be run the next time the computer rebooted."

McAfee, meanwhile, said they identified over 100 unique exploits. And they are still in counting mode.

"McAfee has identified over 100 unique exploits and counting, with most of the initial targets residing in the United States at the time of writing," said Schugar.

Back story: Initially, Check Point Research had reported a discovery of a code execution vulnerability in the WinRAR compression tool. (McAfee described the tool as "wildly popular.") Check Point Research's Nadav Grossman said they found a logical bug. "The exploit works by just extracting an archive," said Grossman. The vulnerability has existed for over 19 years. Result: WinRAR completely dropped support for the vulnerable format.

By now, many computers are at the least aware that mischief makers can be stopped, temporarily, from spreading mischief but the beat goes on for clever attempts to find new ways to transfer malicious code and in a stealthy way where users merrily continue to work unaware of what is happening.

Goodin's take-homes about overall security practices and the WinRAR event: "People should be reflexively suspicious of any file offered for download online. WinRAR users should ensure at once they are using version 5.70. Any other version is vulnerable to these attacks. Another solution is to switch to 7zip."

More information:
www.win-rar.com/whatsnew.html?&L=0
securingtomorrow.mcafee.com/ot … lity-cve-2018-20250/

APA citation: WinRAR patch is issued but the unpatched are at risk (2019, March 19) retrieved 23 October 2021 from https://techxplore.com/news/2019-03-winrar-patch-issued-unpatched.html