Nasty WinRAR bug is being actively exploited to install hard-to-detect malware

reader comments

28 with 22 posters participating

Share this story

Malicious hackers wasted no time exploiting a nasty code-execution vulnerability recently disclosed in WinRAR, a Windows file-compression program with 500 million users worldwide. The in-the-wild attacks install malware that, at the time this post was going live, was undetected by the vast majority of antivirus product.

The flaw, disclosed last month by Check Point Research, garnered instant mass attention because it made it possible for attackers to surreptitiously install persistent malicious applications when a target opened a compressed ZIP file using any version of WinRAR released over the past 19 years. 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. From there, malicious payloads would automatically be run the next time the computer rebooted.

On Thursday, a researcher at McAfee reported that the security firm identified "100 unique exploits and counting" in the first week since the vulnerability was disclosed. So far, most of the initial targets were located in the US.

“One recent example piggybacks on a bootlegged copy of Ariana Grande’s hit album *Thank U, Next* with a file name of ‘Ariana_Grande-thank_u,_next(2019)_[320].rar,’” McAfee Research Architect Craig Schmugar wrote in the post. “When a vulnerable version of WinRAR is used to extract the contents of this archive, a malicious payload is created in the Startup folder behind the scenes. User Access Control (UAC) is bypassed, so no alert is displayed to the user. The next time the system restarts, the malware is run.”

Screenshots included in the post show that the malicious file extracts benign MP3 files to the target’s download folder. Under the hood, however, the RAR file also extracted a file titled “hi.exe” to the startup folder. Once the computer was rebooted, it installed a generic trojan that, according to the Google-owned VirusTotal service, was detected by just nine AV providers. Schmugar didn’t say if all 100 exploits McAfee identified install the same malware.

Web searches such as this one show that an Ariana Grande RAR file with the same title identified by McAfee is currently circulating on BitTorrent download services. They’re also being advertised on Twitter. 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.

https://arstechnica.com/?p=1474331

WordPress 5.1.1 Patches

Remote Code Execution Vulnerability

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/AeDOIqAIggw/wordpress-511-patches-remote-code-execution-vulnerability

---

Code Execution Flaw Found in Sonatype Nexus Repository Manager

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/C4fqOOrlq0s/code-execution-flaw-found-sonatype-nexus-repository-manager

---

Default Account in Cisco CSPC Allows Unauthorized Access

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/rl0EB31RpXI/default-account-cisco-cspc-allows-unauthorized-access

Multiple Security Flaws Discovered in Visitor Management Systems

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/QnPPpgu1aog/multiple-security-flaws-discovered-visitor-management-systems

---

Serious Crypto Flaw Affects Swiss, Australian E-Voting Systems

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/HxxXylOkigc/serious-crypto-flaw-affects-swiss-australian-e-voting-systems

---

Windows Zero-Day Exploited by

FruityArmor, SandCat Threat Groups

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/meoe4MmLxpU/windows-zero-day-exploited-fruityarmor-sandcat-threat-groups

---

Microsoft Patches Two Windows Flaws Exploited in Targeted Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/BOkmHA12EoM/microsoft-patches-two-windows-flaws-exploited-targeted-attacks

---

Senators Reintroduce IoT Cybersecurity Improvement Bill

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/b_reBTbDnKA/senators-reintroduce-iot-cybersecurity-improvement-bill

GIF Attack on Facebook Messenger Earned Hacker $10,000

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/S7jeZizpibU/gif-attack-facebook-messenger-earned-hacker-10000