

Users who have not updated the WinRAR patch, despite being warned, continue to take advantage of the vulnerability to insert malicious code.

WinRAR programmers have released a patch update on version 5.70 beta 1, but because many users do not update to the latest version, the problem is not resolved at the root.

WinRAR, data compression and decompression software, is one of the most popular software for any computer user. Earlier this month, CheckPoint Software's security experts announced a serious vulnerability that lasted 19 years on WinRAR software, and hackers could easily take advantage of it to spread malicious code.

WinRAR programmers have released a patch update on version 5.70 beta 1, but because many users do not update to the latest version, the problem is not resolved at the root. Hackers can continue to take advantage of this vulnerability to embed malicious code in a compressed file, when the user decompresses the malicious code, it will be started and run in the background.

To easily deceive users into downloading and extracting, hackers have embedded malicious code into sexy photos to stimulate their curiosity. Hackers used this flaw to attack Middle Eastern countries or Korean government agencies before the day when the US-Trieu summit took place in Vietnam.



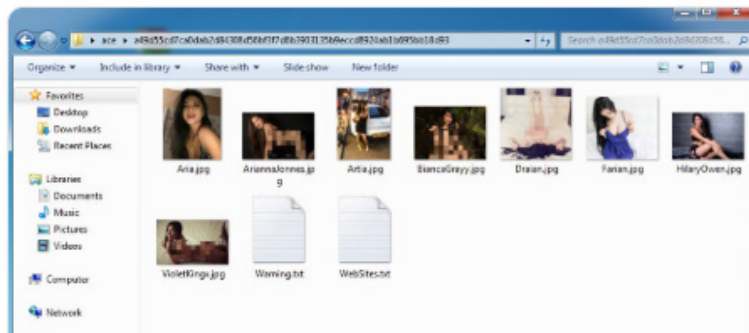
360 Threat Intelligence Center
@360TIC

Follow

Warning! Upgrades in the [#WinRAR](#) vulnerability ([#CVE-2018-20250](#)) exploit, use social engineering to lure victims with embedded image files and encrypt the malicious ACE archive before delivering.

Analysis report: ti.360.net/blog/articles/ ...

Chinese version:
mp.weixin.qq.com/s/hAoe3Z90Fyx...





Once again, security experts recommend users to quickly update to the latest version of WinRAR 5.70 Beta 1 from their official website, and away from ACE-formatted files and image files. Sexy on the Internet to protect yourself.

1. <https://www.win-rar.com/affdownload/download.php>

You finished reading the article "**Users who have not updated the WinRAR patch, despite being warned, continue to take advantage of the vulnerability to insert malicious code.**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.