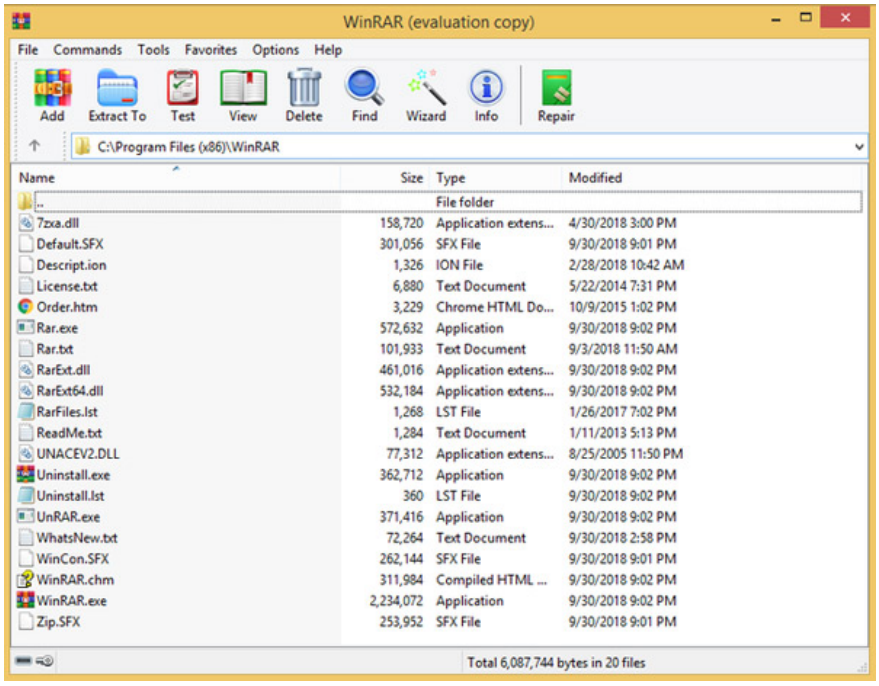
Detecting serious security flaws that exist for more than 19 years on WinRAR, can affect 500 million users

On February 20, security experts at Check Point discovered a very dangerous vulnerability that existed inside the library of WinRAR code over the past 19 years, allowing hackers to broadcast it. A malicious code and plugged into a user's computer to perform malicious purposes.

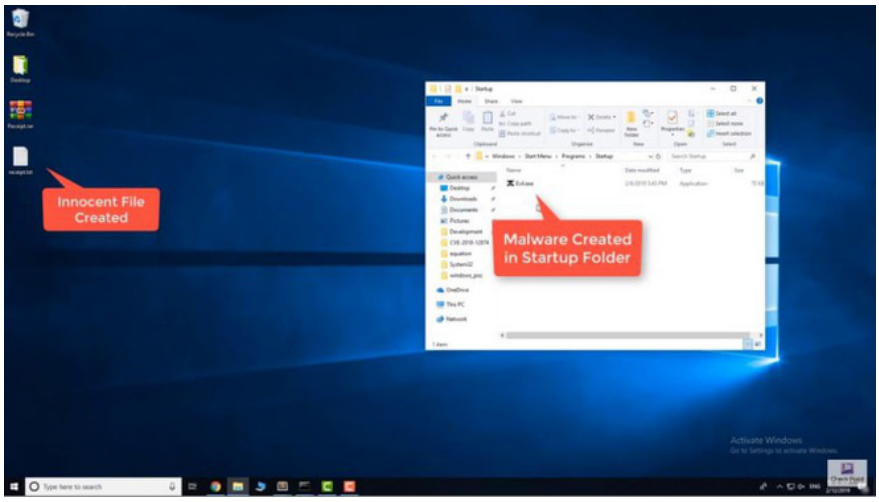
On February 20, security experts at Check Point discovered a very dangerous vulnerability that existed inside the library of WinRAR code over the past 19 years, allowing hackers to broadcast it. A malicious code and plugged into a user's computer to perform malicious purposes. The computers of half a billion WinRAR users may have been affected.

The vulnerability discovered by the experts is in the .dll library file, named "unacev2.dll". If hackers properly exploit this vulnerability, they can take full control of the victim's device. WinRAR uses this file when reading the ACE compression file format. Hacker simply changes the extension of the compressed file (.ACE) to RAR so that it can install malicious code on the victim's computer to hijack, steal data or encrypt the extortion data.



Graphical user interface on WinRAR.

Experts at Check Point have announced this vulnerability for WinRAR. Very quickly, WinRAR released version 5.70 beta 1 to fix this vulnerability.



Check Point uploads an image indicating the malicious file was created inside the user's directory. Currently, users can access the link below to download this patch.

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

You finished reading the article "**Detecting serious security flaws that exist for more than 19 years on WinRAR, can affect 500 million users**" 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.
