Advanced Notification of Cyber Threats against WinRAR ACE Vulnerability

aeCERT
فريق الاستجابة لطوارئ الحاسب الآلي
Computer
Emergency
Response
Team

Security Advisory ADV-19-06 **Criticality** High ○○○●

Advisory Released On 11 March 2019

Impact

A vulnerability in WinRAR that could be exploited by extracting files using WinRAR, and infect users with malware.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms

- Windows Operating System

Summary

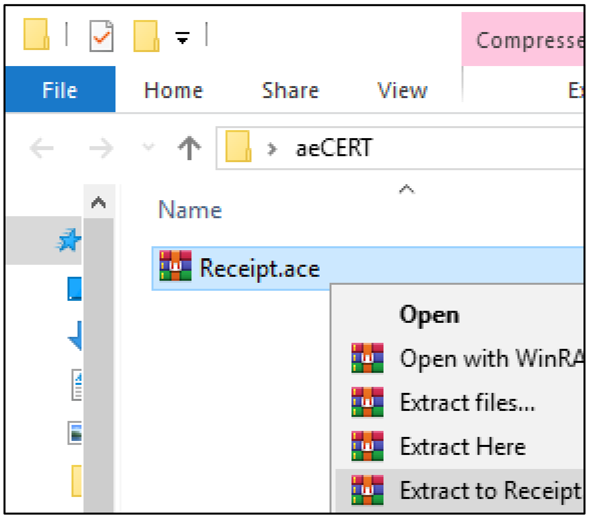
As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered vulnerability currently named as “WinRAR ACE Vulnerability”, with CVE chain of “CVE-2018-20250”, “CVE-2018-20251”, “CVE-2018-20252”, “CVE-2018-20253”. This vulnerability is exploited by the extraction of the obsolete ACE archives through WinRAR. However, attackers may disguise the vulnerable .ACE format into other formats such as .RAR, in order to trick targets. Successful exploitation could result in the attacker to remote code execute a file, such as a malware in arbitrary location. Therefore, extracting files from an archive using WinRAR, could infected users.

Threat Details

WinRAR ACE Vulnerability could permit attackers to remote execute a file in an arbitrary location, giving the possibility to install malwares on vulnerable computers. Thereby, the extraction/ decompression of files from an archive using WinRAR, could infect users.

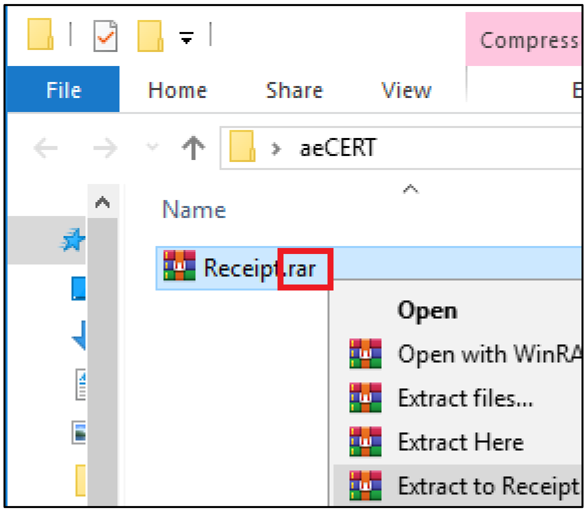
To be thorough, the mentioned vulnerability is exploitable through the decompression/ extraction of the ACE archives using WinRAR. WinRAR featured the decompression of ACE archives using UNACEV2.DLL library, the UNACEV2.DLL library within WinRAR is vulnerable resulting in WinRAR ACE vulnerability. The library is also obsolete and the source code of the library is no longer accessible.

<u>Example showing vulnerable archive of .ace format:</u>



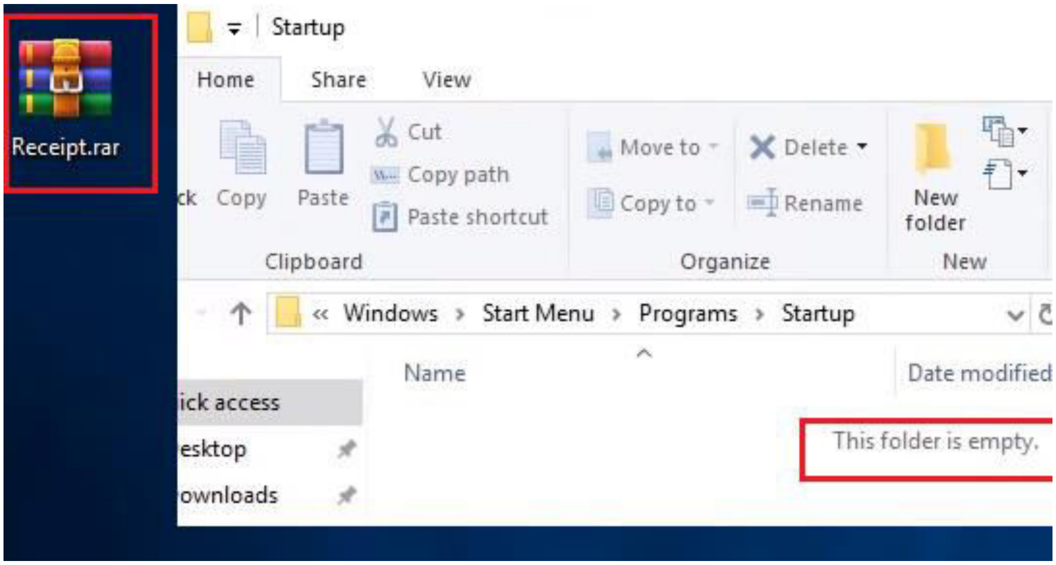
Even though the infection is only possible through the extraction of .ace archives. It is also possible to disguise the vulnerable .ACE format into other formats such as .RAR, in order to trick targets into the extraction of files causing infection.

Example showing disguised vulnerable archive of .ace format as .rar format:

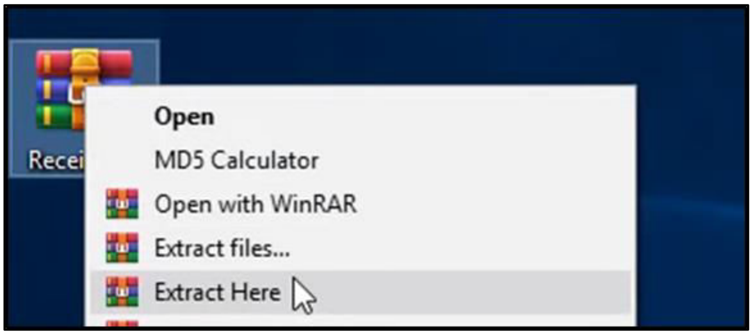


Example showing a disguised malicious archive process:

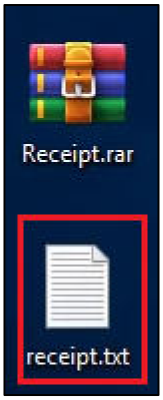
a) Malicious archive targeting empty startup folder



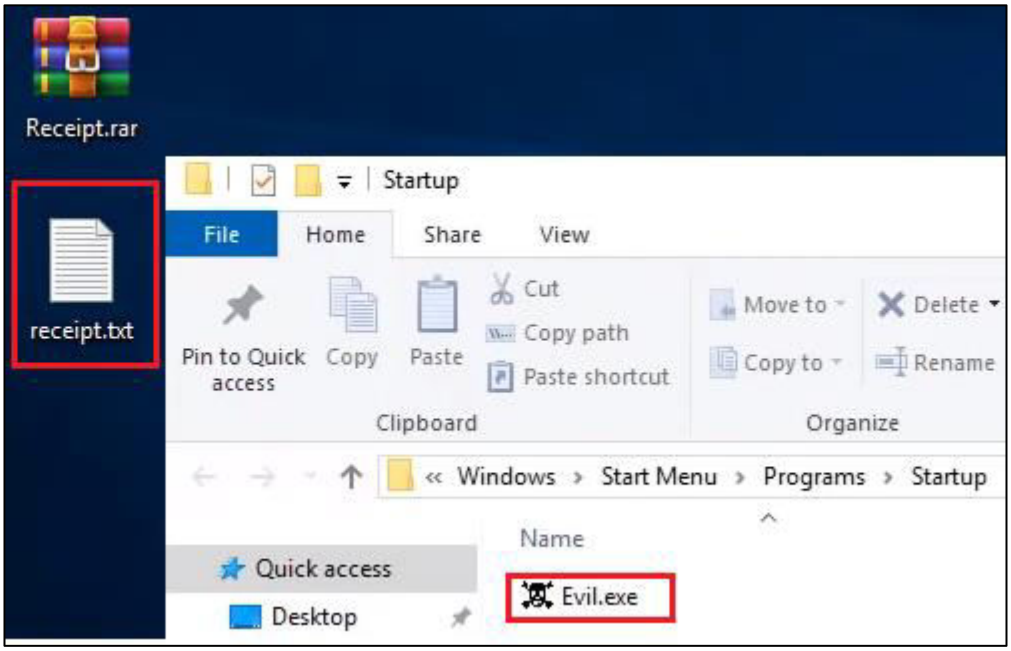
b) **Extracting Receipt.rar in desktop**



c) **Receipt is extracted in desktop**



d) **Malware is also created in the startup folder**



Recommendations

All devices running WinRAR prior to version 5.70 beta 1 are vulnerable and could be exploited. Accordingly WinRAR version 5.70 beta 1 and above has removed the support for ACE format to patch the vulnerability.

To avoid the vulnerability, entities are recommended with the following

- <u>In cases where WinRAR must be installed</u>
    - Update WinRAR to version 5.70 beta 1 and above.
    - If update is not possible, then all devices with WinRAR versions prior to 5.70 beta 1 should avoid the extraction of archives using WinRAR.
- <u>In cases where WinRAR is optional</u>
    - It is recommended to avoid third-party solutions to extract archives, as it is possible to use the built-in Windows Explorer for handling archives.

References

National Vulnerability Database (CVE-2018-20250, CVE-2018-20251, CVE-2018-20252, CVE-2018-20253)

Research Checkpoint

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel	(+971) 4 777 4003
Fax	(+971) 4 777 4100
Email	info[at]aeCERT.ae
Instagram	@TheUAETRA
Twitter	@TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae