**TLP:WHITE**

CERT-EU

# WinRAR zero-day exploited in many attacks

**Reference**: Memo [190401-1] Date: 01/04/2019 - Version: 1.0
**Keywords**: WinRAR, CVE-2018-20250, manual update

**Key Points**

- On February 20, a 20 years old zero-day vulnerability in the archiving software WinRAR, was publicly revealed.
- On February 26, a patched version of WinRAR was released, the update must be done manually.
- More than a hundred unique exploits have been spotted since the publication of proofs of concept and payload creation tools, after the disclosure.

**Description**

Since the end of February, IT security companies have detected several examples of exploitation of a recently discovered zero-day in WinRAR (CVE-2018-20250). On March 26, FireEye provided more context on the global exploitation of this vulnerability and gave a glimpse at the wide range of impacted organisations and sectors. This 20 years old zero-day vulnerability in the archiving utility WinRAR had been publicly revealed on February 20. All versions prior to 5.70 are vulnerable and a patch was released with 5.70 Beta 1 on January 28 (version 5.70 was released on February 26, 6 days after the disclosure).

Technical analysis

The exploitation was possible using a specifically crafted ACE file, disguised as a RAR file. According to the version notes of v5.70 Beta 1, the vulnerability was due to a third party library used for ACE files unpacking, UNACEV2.DLL, that had not been updated since 2005. As RARLAB did not have access to the DLL's code, they decided not to support the ACE format anymore, by removing the DLL from their product in order "to protect security of WinRAR users."

ACE is a proprietary data compression archive file format used in the early 2000', which provided slightly better compression rates than RAR, which has since become more popular.

This exploit allowed an attacker to extract files at the path of their choosing regardless of the extraction process' destination folder. Since the public disclosure, several tools and proofs of concept have emerged and are freely available, which caused the number of attacks to rise quickly.

Exploitation campaigns

According to open sources, at least "100 unique exploits" have been seen after the disclosure. These were aimed at various targets, through spear phishing, including South Korean agencies (prior to the USA / North Korea meeting in Vietnam), Ukrainian citizens (new law themed email), and individuals in Middle-East (using United Nations / human rights as a wrapper for the attack).

In a detailed public blogpost, FireEye listed four campaigns using this newly exposed vulnerability and targeting various sectors:

- Social work education council in the US
- Israeli military industry
- Potential Attack in Ukraine with Empire Backdoor
- Credential and Credit Card Dumps as Decoys

In all cases and in order to ensure the persistence of their attack, the attackers chose to extract malicious files in the Startup folder which allowed the malware to restart with the target computer. All described attacks also used decoy files, related to the theme of the spear phishing, that were contained within the ACE archive in order to diminish the target's suspicion and look as normal as possible. The extracted malicious files are VBScript (.vbs file, with network and payload extraction capabilities), LNK (.bat file, directly pointing to a C2 server IP address, used to fetch the malware itself), another .bat file (containing an instance of the Empire backdoor) and several samples from the Azorult (twice), Netwire, Razy, Buzy and QuasarRAT malware families.

**Comments**

The first version of WinRAR was released 23 years ago, in 1995, and now has over 500 million users worldwide. This makes such type of vulnerability extremely interesting for an attacker as archiving software are used everywhere and sometimes even come preinstalled on new computers as it is the case for WinRAR. This attack surface can be seen as a door to a huge number of systems and enables a wide range of attacks, going from cybercrime to espionage, that can be targeted or have a larger scale.

On the one hand and considering the number of users, the absence of an auto-update feature is somewhat problematic as all versions prior to 5.70 are vulnerable and updates must be done manually. On the other hand and regarding the recent Asus Live Update hack (see MEMO 190326-1), an auto-update feature would have been a particularly interesting target for an actor.

CERT-EU has shared with its constituents actionable threat information related to this attack via its usual threat data sharing channels. CERT-EU further advises to update WinRAR to its latest version. The update policy for utility software should also be reviewed in the light of the recent events and their security implications. For more information regarding this threat, please contact CERT-EU.

**Sources:** FireEye, other open sources.