



Cytex Research

CVE-2023-4047

Remote Code Execution Vulnerability

WinRAR RCE Vulnerability Advisory

hello@cytex.io | <https://cytex.io>

1

What is the WinRAR Remote Code Execution Vulnerability?

WinRAR is a popular program to handle different types of compressed files. Its versatile functionality has made it quite popular and there are over 500 million installations worldwide.

Recently, a critical security vulnerability CVE-2023-40477 was discovered in WinRAR versions 6.22 and lower. This vulnerability allows an attacker to take over a computer through remote code execution by simply convincing a user to open an infected file. The root cause of this vulnerability lies in improper validation of user supplied data. An attacker can craft a data file that leads to a buffer overflow in the memory, which creates a potential for remote code execution. After an attacker takes over the computer, they may execute arbitrary code without the user knowing about it.

Vulnerability

Remote Code Execution Vulnerability

CVE

CVE-2023-40477

CVSS Score

7.8 out of 10

Security Level

High

Affected Product

WinRAR v6.22 or lower



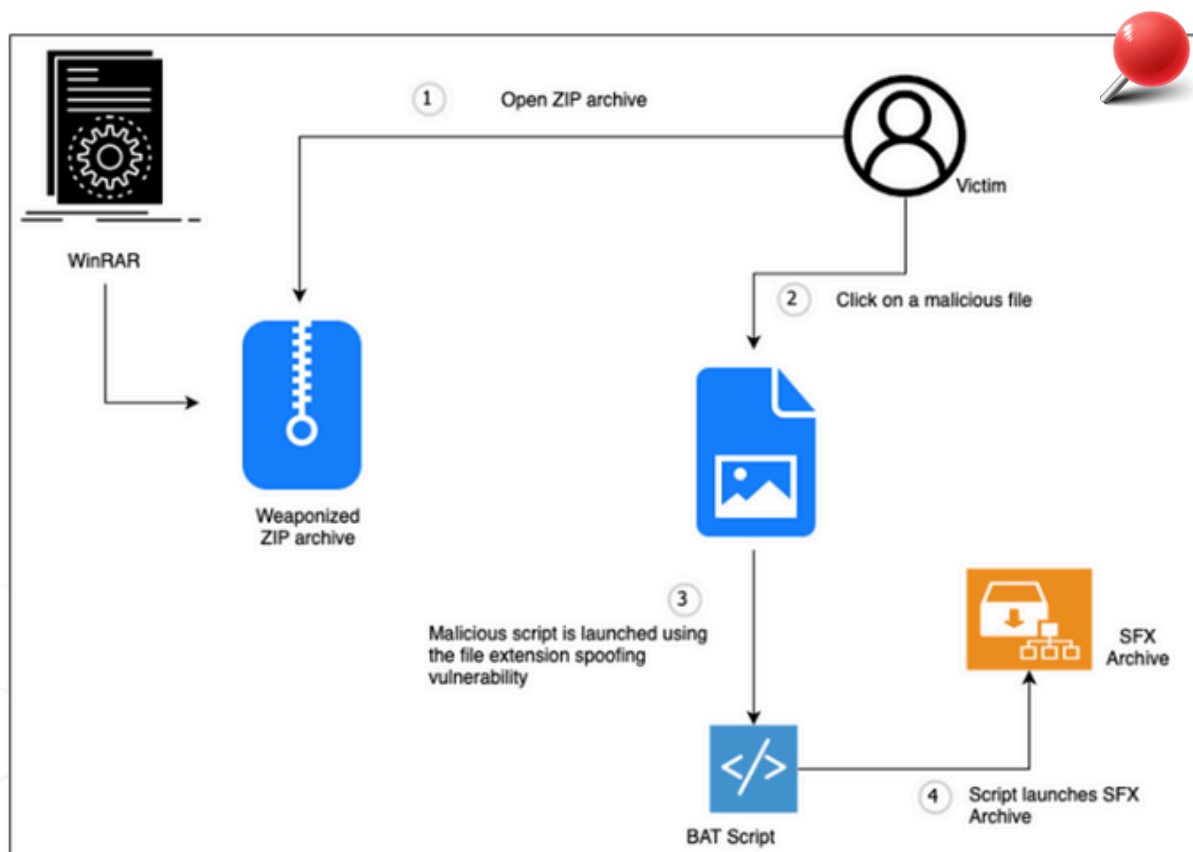
LowCritical

2

How does the WinRAR vulnerability work?

Through the WinRAR vulnerability, attackers have managed to weaponize ZIP files into carriers of malware. Malicious ZIP archives were posted on public forums frequented by traders to swap information and discuss topics related to cryptocurrencies and other securities. In most cases, the ZIP archives were attached to forum messages, but there have also been reported cases of infected files being distributed through file sharing services.

Attackers are exploiting a vulnerability that allows them to spoof file extensions within an archive by masquerading as '.jpg', '.txt', or other formats. When a victim opens a specially crafted file, they see an image file and a folder with the same name. If the victim clicks on the decoy file, it launches a script that initiates the next phase of the attack.



3 How do I know if I am at risk?

If you use WinRAR version 6.22 or lower, then you are at risk.

4 What should I do?

You should immediately take these steps:

- Identify and remove the vulnerable WinRAR version. Upgrade to v6.23 or higher if you would like to continue and use WinRAR
- Educate your employees about the dangers of opening files sent by strangers
- Restrict access to sites where attackers may convince users to accept malicious files by disguising them as investment advice or other innocuous topics
- Keep your operating system and application software up to date

4.1 Identify vulnerable software

Identify all devices that have WinRAR v6.22 or lower installed. If you are running Cytex EDR, you can easily identify the devices that have WinRAR v6.22 or lower, installed and remove the affected version.

You should also use the Cytex EDR to identify any vulnerable software installed on managed devices and immediately update to the latest version.



Identify & remove the vulnerable WinRAR version v6.22 or lower. Upgrade to v6.23 or higher if you would like to continue and use WinRAR.



Train your employees not to open unsolicited email or to download files or click on links from senders they don't recognize.

4.1 Identify vulnerable software

If you are not a Cytex EDR customer, you can use these instructions to identify and remove the vulnerable version.

- 1. Open a command window
- 2. Type %APPDATA%
 - If WinRAR is installed, its installed folder will be displayed
- 3. Remove the vulnerable WinRAR from the Add/Remove Software section
- Verify that WinRAR has been removed and the folder is removed

4.2 Employee Awareness Training

If you are a Cytex customer, you can use the Cytex Security Training module to educate employees about social engineering attacks as well as the risks of running vulnerable software. Cytex provides several modules that address these topics. Employees can consume the easy-to-read content and then take a short quiz to test their understanding of the material.

If you are not a Cytex customer, you can use education content offered by FTC: <https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security> to educate your employees about the risks of malware and social engineering attacks.



cytex-inc



@cytexsmb



@cytexsecure