Introduction

We have received many questions from software developers and WinRAR users about the CVE-2023-40477 vulnerability. We would like to provide more details here.

Description

A buffer overflow is possible when processing recovery volume names in the old RAR 3.0 format. The user must start unpacking a RAR file in the same folder as a REV file with a malformed name to trigger this vulnerability. This has been fixed in WinRAR 6.23.

Are the UnRAR.dll and UnRAR64.dll vulnerable?

Unlike the WinRAR.exe, RAR.exe and UnRAR.exe executables, the original unrar.dll and unrar64.dll libraries provided on our site are not vulnerable. We can see that the UnRARDll.vcxproj project file in unrarsrc-6.2.8.tar.gz doesn't include the affected recvol3.cpp file and that the RecVolumesRestore() function is not called if the RARDLL preprocessor variable is defined. This variable is defined when building the unrar.dll and unrar64.dll.

We have chosen UnRAR source code 6.2.8 as a sample, because it is the last UnRAR version without a fix for this vulnerability. Older versions of UnRAR source code also do not call the recovery volume processing code for unrar.dll and unrar64.dll.

Is there proof of concept for remote code execution?

We do not have such a proof of concept archive. The buffer border is overwritten with pointers to objects returned by the C++ *new* operator. This makes it difficult for an attacker to control the contents of data written beyond the buffer border. It also makes it difficult to implement a remote code execution exploit. While we can't claim that it is impossible, all we've seen so far is a denial-of-service, or in other words, an application crash that doesn't lead to code execution, overwriting of system files, or other serious security implications.

When will the CVE record be updated with the latest information?

CVE record is created and maintained by researchers at the Zero Day Initiative. win.rar GmbH is not involved in the process of updating the CVE record.