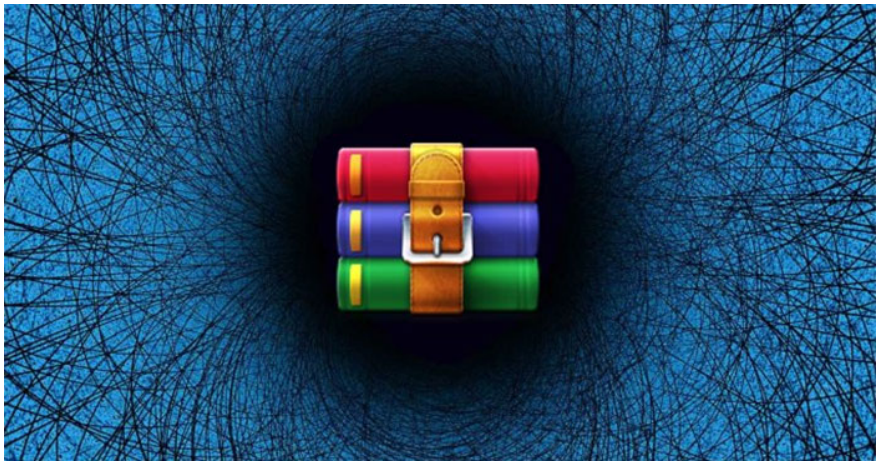
WinRAR releases emergency patch for serious security vulnerability, users need to update immediately

Last week, WinRAR version 7.13 was released, fixing a directory traversal vulnerability, tracked under the identifier CVE-2025-8088.

Last week, WinRAR version 7.13 was released, fixing a directory traversal vulnerability, which is tracked as CVE-2025-8088. Thanks to researchers from ESET, we now have more details on how to exploit this vulnerability, especially since some hacker groups are actively using it for malicious purposes.

Specifically, this vulnerability lies in the core library UNRAR.dll, which is responsible for decompressing files. Hackers create a malicious compressed file that can 'trick' the software into writing files to a location of their choice instead of the folder specified by the user.

When unpacking, earlier versions of WinRAR, WinRAR on Windows, UnRAR, UnRAR portable source code and UnRAR.dll can be tricked into using a path defined in a special archive instead of a user-selected path.



According to ESET experts Anton Cherepanov, Peter Košinár, and Peter Strý?ek, attackers exploit this vulnerability to insert payloads into sensitive locations in the system, such as the Startup folder. By placing an executable file in **%APPDATA%MicrosoftWindowsStart MenuProgramsStartup** , the malicious code will automatically run when the user logs in, allowing hackers to execute code remotely on the compromised machine.

The group behind these attacks is believed to be the 'RomCom crew'. The RomCom malware is a Remote Access Trojan (RAT) that has been active since at least 2022. It uses social engineering to trick users, even impersonating popular software websites like KeePass, to trick victims into downloading the RAT installer. This hacking group has primarily targeted countries like Ukraine and some NATO members.

This is not the first time WinRAR has faced a serious security issue this year. Previously, version 7.12 patched a similar vulnerability (CVE-2025-6218) that affected WinRAR 7.11 and earlier versions.

According to Bleeping Computer, WinRAR does not have a built-in automatic update mechanism, so users must proactively access the official website to download and install version 7.13 to ensure safety. WinRAR also confirmed that the Unix versions of RAR and UnRAR, along with RAR for Android, will not be affected.