

Warning of dangerous vulnerabilities on WinRAR, users should uninstall or upgrade to a new version

RARLAB, the developer of WinRAR, has just released an urgent update to patch a dangerous vulnerability in their software.

RARLAB, the developer of WinRAR, has just released an urgent update to patch a dangerous vulnerability in their software. This vulnerability was discovered by researcher Igor Sak-Sakovskiy. Tracked with the code CVE-2021-35052, the WinRAR vulnerability has a large scope of impact.

WinRAR is a popular file compression and decompression software, widely used on personal computers and also in offices and businesses. Therefore, if hackers successfully exploit the CVE-2021-35052 vulnerability, the consequences they cause will be very heavy.



The vulnerability stems from WinRAR using insecure connections to access message content from the server side through Notifer Windows. Therefore, an attacker can penetrate this connection to install malicious code on the victim's machine to gain control. Moreover, hackers can also attack multiple targets at the same time to create large-scale targeted attack campaigns.

WinRAR has released update 6.02 to patch CVE-2021-35052.

For users, you can keep yourself safe by updating WinRAR. Alternatively, you can also completely remove this software from your computer and replace it with a better file compression and decompression software, such as 7zip.

You finished reading the article "**Warning of dangerous vulnerabilities on WinRAR, users should uninstall or upgrade to a new version**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
