



**NATIONAL
CSIRT CY**



WinRAR path traversal vulnerability affecting v7.12

12/08/2025

(CVE-2025-8088)

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

ESET researchers discovered a path traversal vulnerability affecting WinRAR v7.12

The vulnerability exploits alternate data streams (ADSs) to achieve path traversal.

The malicious actors craft special archives that have within them malicious ADSes.

We urge everyone to as soon as possible upgrade to the latest version from WinRAR.

Indications show that there is an active campaign exploiting this vulnerability

Affected Products

WinRAR v7.12

Common Weakness Enumeration

<https://cwe.mitre.org/data/definitions/35.html>

Common Vulnerabilities & Exposures

<https://nvd.nist.gov/vuln/detail/CVE-2025-8088>

Solutions

Make sure you are using the latest version of WinRAR and not v7.12 or less.

https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=283&cHash=a64b4a8f662d3639dec8d65f47bc93c5

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.