CAA-2026-0004 WinRAR High-Severity Vulnerability Continues to be Actively Exploited

Summary

On 27 January 2026, Google Threat Intelligence Group (GTIG) identified the active exploitation of CVE-2025-8088 by multiple government-backed threat actors linked to Russia and China, and financially motivated threat actors. CVE-2025-8088 is a path traversal vulnerability affecting Windows versions of WinRAR prior to 7.13.

Although a patch was released on 30 July 2025, CVE-2025-8088 continues to be actively exploited.

Details

CVE-2025-8088 (CVSS 8.4) is a path traversal vulnerability affecting the Windows version of WinRAR that can execute arbitrary code in specially-crafted archive files.[1] ESET researchers observed the initial exploitation of this vulnerability on 18 July 2025 by a Russian-nexus group.[2] RARLAB subsequently released WinRAR version 7.13 on 30 July 2025 to address the vulnerability. However, nation-state threat actors from Russia and China, and cybercriminals, continue to exploit CVE-2025-8088 for both espionage and financial gain.

According to GTIG, the exploit chain leverages NTFS Alternate Data Streams (ADS) to conceal malicious executable and the path traversal vulnerability to write files to an auto-start location. The victim receives a `.rar` file archive containing a decoy document—such as a PDF—while additional ADS entries hide the malicious payload. Upon the user opening and extracting the malicious `.rar` file archive, the directory traversal vulnerability writes the payload to an auto-start folder, such as the user's `Startup`[3]. This allows the threat actor to establish persistence on the system and the payload is executed by Windows during user login, without the user observing any sign of compromise.

Unmanaged software represents an attractive attack surface for threat actors, particularly in small and medium-sized organizations where users often install applications outside of IT oversight. Applications like WinRAR are commonly treated as utility software rather than enterprise assets, resulting in inconsistent patching, limited visibility, and prolonged exposure to known vulnerabilities.

The campaigns exploiting CVE-2025-8008 were typically highly targeted, using geopolitical or regionally relevant lures to increase credibility and engagement.[4] This activity was directed at employees whose roles require frequent opening, sharing, and handling of compressed files as part of routine business operations. This makes exploitation more likely to succeed without triggering suspicion, allowing attackers to gain an initial foothold through otherwise normal user behavior.

[1] https://nvd.nist.gov/vuln/detail/CVE-2025-8088
[2] https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
[3] https://cloud.google.com/blog/topics/threat-intelligence/exploiting-critical-winrar-vulnerability
[4] https://research.checkpoint.com/2026/amaranth-dragon-weaponizes-cve-2025-8088-for-targeted-espionage/

Assessment

CyberAlberta Threat Intelligence assesses that unpatched WinRAR versions are highly susceptible to exploitation. Organizations that do not maintain software inventory, patch management, or endpoint controls face increased risk of compromise and persistent access.

Recommendations

- Immediately patch WinRAR to version 7.13 or later.
- Establish and maintain an up-to-date software inventory, track installed applications to ensure visibility into potential attack surfaces.
- Restrict the installation and execution of unmanaged applications.
- Educate users on the risks of opening unexpected archives and documents.

MITRE ATT&CK

The following table maps tactics, techniques, and procedures (TTPs) described in this report to the MITRE ATT&CK Framework.

Tactic	Technique	Observable
Initial Access	T1566.001 – Phishing: Spearphishing Attachment	Delivers a malicious RAR archive as an attachment, often using targeted geopolitical-themed lures.
Execution	T1204.002 – User Execution: Malicious File	Requires the user to open and extract a file from the RAR archive.
Persistence	T1037.005 – Boot or Logon Initialization Scripts: Startup Items	The attack writes a malicious file to a Windows startup path, automatically executing the payload during user login.
Defense Evasion	T1564.004 – Hide Artifacts: NTFS File Attributes	The malicious payload is hidden within an NTFS Alternate Data Stream (ADS).

Table 1. CVE-2025-8088 Exploitation TTPs