مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Zero-Day Vulnerability in WinRAR

Tracking #:432317586

Date:11-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a zero-day path traversal vulnerability in the Windows version of WinRAR, actively exploited to execute arbitrary code on victim systems.

TECHNICAL DETAILS:

A **zero-day path traversal vulnerability** in the Windows version of WinRAR is being actively exploited to execute arbitrary code on victim systems. The flaw, tracked as **CVE-2025-8088**, allows specially crafted archives to manipulate the extraction process, placing malicious files in unintended system locations without user awareness.

Vulnerability Details:

- **CVE-2025-8088**
- CVSS Score 8.4 High
- When extracting a malicious archive, vulnerable versions of WinRAR may honor attacker-controlled embedded file paths instead of the user's chosen destination folder. This flaw affects multiple Windows-based components, including RAR, UnRAR, the portable UnRAR source code, and UnRAR.dll

Impact

Exploitation could allow attackers to:

- Plant malicious files in sensitive directories.
- Overwrite critical system or application files.
- Execute arbitrary code upon extraction without additional user interaction.

Attackers have been observed delivering malicious archives via phishing and other social engineering tactics.

Affected Products:

- Windows versions of WinRAR (including previous releases of RAR, UnRAR, portable UnRAR source code, and UnRAR.dll)

Fixed Versions:

- WinRAR 7.13 or later

RECOMMENDATIONS:

- Update immediately to WinRAR 7.13 or later from the official WinRAR website.
- Avoid opening archives from untrusted or unknown sources.
- Scan archives with updated endpoint security tools before extraction.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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