مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Vulnerability in WinRAR

Tracking #:432317033

Date:03-04-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in WinRAR that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

A critical security vulnerability, tracked as CVE-2025-31334, exists in WinRAR, a widely used file compression utility. This vulnerability allows attackers to bypass the Windows Mark-of-the-Web (MotW) security feature, enabling the execution of arbitrary code without user warnings.

Vulnerability Details:

- CVE-2025-31334
- CVSS Score: 6.8 Medium
- The vulnerability stems from how WinRAR processes symbolic links within .rar archives. Attackers can craft malicious .rar archives containing symlinks that point to executable files. When a user extracts and opens these symlinks using a vulnerable version of WinRAR, the associated executable is launched without the standard Windows MotW security prompt.
- Successful exploitation of this vulnerability can lead to:
    - Malware installation (viruses, ransomware, spyware)
    - Data theft (personal information, passwords, financial data)
    - Remote system access
    - System damage (corruption or deletion of critical files)
- Attack Vector: Attackers can distribute malicious .rar archives via various methods, including email attachments, malicious websites, and other file-sharing platforms.

Affected Versions:

- All WinRAR versions prior to 7.11

Fixed Versions:

- WinRAR to version 7.11 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by WinRAR.

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-2025-31334