مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

RCE Vulnerability in WinRAR

Tracking #:432317407

Date:24-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a newly disclosed vulnerability in RARLAB's WinRAR, the long-standing compression utility for Windows, exposing millions of users to a severe directory traversal flaw that could lead to remote code execution (RCE).

TECHNICAL DETAILS:

A critical security vulnerability, tracked as **CVE-2025-6218** and rated **CVSS 7.8**, could allow an attacker to run arbitrary code on a victim's machine simply by getting them to open a specially crafted archive file. The malicious payload is typically disguised as a legitimate archive, hiding the exploit within seemingly harmless content.

The flaw lies in insufficient validation when extracting archive entries, specifically failing to properly sanitize crafted path values. By including directory traversal sequences (like ../) in a file's path, an attacker can cause WinRAR to extract files to unexpected locations on the victim's system.

Vulnerability Details:

- CVE ID: CVE-2025-6218
- Severity: High (CVSS 7.8)
- Impact: Remote Code Execution
- Affected Versions:
  - < WinRAR 7.12 Beta 1
- Fixed Versions:
  - WinRAR 7.12 Beta 1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to organizations using WinRAR should upgrade to the latest patched versions.

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://www.zerodayinitiative.com/advisories/ZDI-25-409/