مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in WinZip

Tracking #:432316868

Date:14-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in WinZip that can be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-1240**
- CVSS Base Score: 7.8 HIGH
- A security vulnerability exists in WinZip that could allow remote attackers to execute arbitrary code on affected installations. Exploiting this vulnerability requires user interaction, such as opening a malicious file or visiting a compromised web page.
- The vulnerability exists due to improper validation of user-supplied data when parsing 7Z archive files. Specifically, an out-of-bounds write issue occurs, allowing an attacker to write data past the allocated buffer. By leveraging this flaw, an attacker can execute arbitrary code within the context of the current process.
- Successful exploitation could lead to:
  - Full system compromise
  - Installation of malware or ransomware
  - Theft of sensitive data
  - Lateral movement within networks

Affected Versions:

- WinZip versions prior to 29.0

Fixed Versions:

- WinZip 29.0 or later

RECOMMENDATIONS:

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

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-25-047/