مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in 7-Zip

Tracking #:432316552

Date:25-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in 7-Zip that could potentially be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-11477**
- CVSS Score: 7.8 (High)
- A security vulnerability has been identified in the popular file archiver 7-Zip. This vulnerability allows remote attackers to execute arbitrary code on affected systems by exploiting an integer underflow in the Zstandard decompression function.
- The vulnerability can be exploited by tricking users into opening maliciously crafted archive files, potentially leading to data theft or complete system compromise. Interaction with the library is necessary for exploitation, but the attack vectors may vary depending on implementation.

Affected Versions:

- 7-Zip Versions prior to 24.07

Fixed Versions:

- 7-Zip version 24.07 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-11477