مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Heap-Based Buffer Overflow Vulnerability in 7-Zip

Tracking #:432319307

Date:17-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a heap-based buffer overflow vulnerability has been disclosed in 7-Zip that could allow an attacker to execute arbitrary code.

TECHNICAL DETAILS:

A heap-based buffer overflow vulnerability has been disclosed in 7-Zip, one of the world's most widely used file archiving utilities. Tracked as CVE-2026-14266, the flaw affects the processing of XZ-compressed data and could allow an attacker to execute arbitrary code by convincing a user to open a specially crafted archive file.

Vulnerability Details:

- CVE ID: CVE-2026-14266
- Vulnerability: Heap-Based Buffer Overflow in XZ Decompression
- CVSS v3.1 Score: 7.0 (High)
- CVSS Vector: AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
- Affected Product: 7-Zip
- Affected Versions: All versions prior to 7-Zip 26.02
- Fixed Version: 7-Zip 26.02
- Attack Vector: Local (requires user interaction)
- Privileges Required: None
- User Interaction: Required
- Authentication Required: No

RECOMMENDATIONS:

Immediate Actions:

- Upgrade 7-Zip version to fixed version or later.

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-26-444/