مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in 7-Zip

Tracking #:432319025

Date:26-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a heap buffer overflow vulnerability in 7-Zip. The vulnerability could allow remote attackers to execute arbitrary code or cause affected systems to crash by tricking users into opening specially crafted archive files.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-48095**
- **Severity:** High | **CVSS:** 8.8
- The vulnerability exists in the NTFS archive handler of 7-Zip due to improper memory allocation during processing of crafted NTFS compressed streams. A specially crafted archive can trigger a heap buffer overflow, resulting in memory corruption and potential arbitrary code execution through vtable hijacking techniques.
- The flaw can be exploited using malicious files disguised as common archive formats such as .7z, .zip, or .rar, as 7-Zip performs signature-based archive detection.
- A public proof-of-concept (PoC) is available, increasing the risk of exploitation.

Affected Version

- 7-Zip - All versions through 26.00 are affected.

Fixed Versions

- 7-Zip version 26.01 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by 7-Zip.

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://securitylab.github.com/advisories/GHSL-2026-140_7-Zip/