مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

7-Zip Mark-of-the-Web Bypass Vulnerability

Tracking #:432316765

Date:21-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high severity vulnerability has been discovered in 7-Zip, a widely-used file archiver tool, which could allow attackers to bypass Windows' Mark-of-the-Web security feature.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-0411) has been discovered in 7-Zip, a popular file archiving utility. This flaw allows attackers to bypass the Windows "Mark-of-the-Web" (MotW) security feature, potentially enabling the execution of malicious code without user warning.

CVE-2025-0411 is a protection mechanism bypass vulnerability in 7-Zip that affects its handling of archived files. When extracting files from a crafted archive bearing the Mark-of-the-Web, vulnerable versions of 7-Zip fail to propagate this security indicator to the extracted files.

- CVE Identifier: CVE-2025-0411
- CVSS Score: 7.0 (High)
- Vulnerability Type: Code Execution, Bypass Security Feature
- Affected Product: 7-Zip (versions prior to 24.09)

Impact

- Execute arbitrary code with user privileges
- Bypass Windows security measures designed to protect against untrusted files.
- Potentially deliver and execute malware without triggering standard security warnings.

Fixed Versions:

- 7-Zip version 24.09

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update 7-Zip version to fixed version or later across all systems.

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-25-045/