

CVE-2025-0411

7-Zip Mark of the Web Bypass Vulnerability

CISA KEV since Feb 6, 2025

Actively exploited

7-Zip Mark-of-the-Web Bypass Vulnerability. This vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of archived files. When extracting files from a crafted archive that bears the Mark-of-the-Web, 7-Zip does not propagate the Mark-of-the-Web to the extracted files.

EVRS 76/₁₀₀ Urgent priority	CVSS V3.1 7.0 High · NVD	EPSS 0.671 99.3rd percentile · FIRST	CISA DEADLINE Feb 27, 2025 KEV since 2025 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.671 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

An attacker can leverage this vulnerability to execute arbitrary code in the context of the current user. Was ZDI-CAN-25456.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
active iq unified manager	–	no fixed version listed	NVD
7-zip	< 24.09	24.09	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2pjj-wvcg-vhr8
NVD nvd.nist.gov/vuln/detail/CVE-2025-0411
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-1658

7-zip.org 7-zip.org/history.txt
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-0411

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.