مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Path Traversal Vulnerability in npm Package

Tracking #:432319290

Date:13-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the @xhmikosr/decompress npm package.

TECHNICAL DETAILS:

A critical vulnerability, CVE-2026-53486 (CVSS 9.1 - Critical), has been identified in the @xhmikosr/decompress npm package, a widely used JavaScript library for extracting compressed archives. The flaw allows specially crafted archive files to write files, create symbolic links (symlinks), or hard links outside the intended extraction directory, potentially resulting in arbitrary file overwrite, privilege escalation, or remote code execution depending on the execution environment.

Vulnerability Details:

- CVE ID: CVE-2026-53486
- CVSS Score: 9.1 (Critical)
- CVSS Version: CVSS v3.x
- Vulnerability Type: Path Traversal / Arbitrary File Write
- Affected Product: @xhmikosr/decompress (npm package)
- Affected Versions:
  - Earlier than 10.2.1
  - 11.0.0 through 11.1.2
  - Legacy decompress releases up to 4.2.1 (unmaintained)
- Patched Versions:
  - 10.2.1
  - 11.1.3 and later

RECOMMENDATIONS:

Immediate Actions:

- Upgrade @xhmikosr/decompress to fixed version.

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://github.com/XhmikosR/decompress/security/advisories/GHSA-mp2f-45pm-3cg9