مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in tar-fs NPM package

Tracking #:432317614

Date:19-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the widely used tar-fs NPM package. The flaw could allow attackers to manipulate tar archive extraction in a way that enables arbitrary file writes outside the intended directory, potentially leading to data compromise or system takeover.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-48387 – Directory Traversal via Malicious Tar Files**
- **Severity**: Critical
- **Proof-of-concept (PoC)**: Available
- A security vulnerability exists in the tar-fs NPM package that allows attackers to perform directory traversal attacks using malicious tar files. The flaw enables arbitrary file writes outside the designated extraction directory, potentially leading to data corruption, privilege escalation, or remote code execution.

Affected Versions:

- tar-fs < 3.0.8
- tar-fs < 2.1.2
- tar-fs < 1.16.4

Fixed Versions:

- tar-fs v3.0.9
- tar-fs v2.1.3
- tar-fs v1.16.5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed or latest security updates released by the vendor.

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/google/security-research/security/advisories/GHSA-xrg4-qp5w-2c3w