مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache MINA

Tracking #:432319098

Date:09-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache MINA. These vulnerabilities could allow attackers to bypass deserialization security controls and trigger denial-of-service (DoS) conditions through excessive memory consumption. Successful exploitation may impact the security, stability, and availability of affected applications.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-47065**
  - **Severity:** Critical
  - A deserialization vulnerability exists in Apache MINA's object deserialization process. The issue allows attackers to bypass configured class allow-lists through Java Proxy class handling and trigger the static initialization of allow-listed classes during deserialization. Successful exploitation could bypass security restrictions and execute unintended code paths within affected applications.
- **CVE-2026-47321**
  - A flaw in the CompressionFilter component allows specially crafted compressed data to expand excessively during decompression, potentially causing memory exhaustion and denial of service (DoS).

Fixed Versions

- Apache MINA 2.0.29
- Apache MINA 2.1.13
- Apache MINA 2.2.8

For environments utilizing the CompressionFilter feature, Apache recommends configuring decompression limits using the newly introduced parameters such as maxDecompressedSize, maxDecompressRatio, and decompressRatioMinSize to mitigate decompression amplification attacks.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache MINA.

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://lists.apache.org/thread/y7xj1bl8qo47p9bktb11hg5v6k1d4dyj