



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical RCE Vulnerabilities in Apache MINA

Tracking #:432318890

Date:04-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Apache MINA. These flaws impact Java object deserialization protections and could allow unauthenticated attackers to execute arbitrary code on vulnerable systems through crafted network input.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-42778**
 - **Severity:** Critical | **CVSS:** 9.8
 - An incomplete fix in `IoBuffer.getObject()` caused the classname allowlist security check to be enforced only after malicious classes were already loaded. Attackers could supply crafted serialized objects that trigger execution of a malicious class's static initializer before the allowlist rejected it, enabling unauthenticated remote code execution.
- **CVE-2026-42779**
 - **Severity:** Critical | **CVSS:** 9.8
 - A logic flaw in `AbstractIoBuffer.resolveClass()` allowed a specific code path for static classes or primitive types ("null-clazz" branch) to bypass the `acceptMatchers` security filter entirely. This bypass enabled attackers to deserialize arbitrary Java classes over the network, leading to full unauthenticated remote code execution.

Affected Versions

- Apache MINA 2.1.0 to 2.1.11
- Apache MINA 2.2.0 to 2.2.6

Fixed Versions:

- Apache MINA 2.1.12 or later
- Apache MINA 2.2.7 or later

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/fhlx5k91hrkgyzh7yk1nghrn3k27gxy0>