مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerabilities in Apache MINA

Tracking #:432318852

Date:28-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that two critical vulnerabilities—CVE-2026-41635 and CVE-2026-41409—have been identified in Apache MINA, a widely used Java-based network application framework.

TECHNICAL DETAILS:

Two critical vulnerabilities—CVE-2026-41635 and CVE-2026-41409—have been identified in Apache MINA, a widely used Java-based network application framework. Both flaws carry a CVSS score of 9.8 (Critical) and enable Remote Code Execution (RCE) via unsafe deserialization mechanisms.

Vulnerability Details:

1. **CVE-2026-41635 – Allowlist Bypass in Deserialization**
   - Severity: Critical (CVSS 9.8)
   - Type: Improper Input Validation / Logic Flaw
   - Root Cause:
     - In AbstractIoBuffer.resolveClass(), certain execution branches (e.g., static classes or primitive types) do not enforce classname allowlist checks.
   - Impact:
     - Attackers can craft serialized payloads that bypass validation.
     - Enables execution of arbitrary classes leading to RCE.
   - Attack Vector:
     - Remote, unauthenticated (depending on application exposure).
   - Key Issue:
     - Inconsistent enforcement of acceptMatchers filter.

2. **CVE-2026-41409 – Delayed Allowlist Enforcement (Incomplete Fix)**
   - Severity: Critical (CVSS 9.8)
   - Type: Unsafe Deserialization / Improper Initialization Order
   - Root Cause:
     - Allowlist validation is applied after class loading.
     - Java executes static initializers upon class loading, before validation.
   - Impact:
     - Malicious code embedded in static blocks executes before security checks.
     - Leads to pre-validation RCE.
   - Attack Vector:
     - Remote exploitation via crafted serialized objects.
   - Key Issue:
     - Incomplete remediation of prior vulnerability (CVE-2024-52046).

Affected Versions

- 2.2.x: 2.2.0 → 2.2.5
- 2.1.x: 2.1.0 → 2.1.10
- 2.0.x: 2.0.0 → 2.0.27

Fixed Versions

- 2.0.28
- 2.1.11
- 2.2.6

RECOMMENDATIONS:

- Upgrade Immediately: Upgrade Apache MINA to patched versions.

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://nvd.nist.gov/vuln/detail/CVE-2026-41635
- https://nvd.nist.gov/vuln/detail/CVE-2026-41409