



# Apache MINA: AbstractIoBuffer.resolveClass() null-clazz Branch Skips acceptMatchers Filter — Full Object Deserialization RCE

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-41635
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 09:16:01 UTC
<b>Updated</b>	2026-04-29 19:08:21 UTC
<b>Description</b>	Apache MINA's AbstractIoBuffer.resolveClass() contains two branches, one of them (for static classes or primitive types) dc

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from security@apache.org

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000460000 probability, percentile 0.140610000 (date 2026-04-27)

**Problem Types:** CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	security@apache.org	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Mina	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache MINA	affected 2.2.0 2.2.5 semver	Not specified
CNA	Apache Software Foundation	Apache MINA	affected 2.1.0 2.1.10 semver	Not specified
CNA	Apache Software Foundation	Apache MINA	affected 2.0.0 2.0.27 semver	Not specified

### References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/27/4	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List,
lists.apache.org/thread/1191w1mqsb3lwfd504fs045ylxntt2tm	security@apache.org	<a href="http://lists.apache.org">lists.apache.org</a>	Mailing List,
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

### Vendor Comments And Credit

Discovery Credit

**CNA:** Venkatraman Kumar, Securin (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-17T00:00:00.000Z	Initial reporting

There are currently no legacy QID mappings associated with this CVE.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)