



# CVE-2016-3973

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-3973                                                                                                              |
| State           | PUBLISHED                                                                                                                  |
| Assigner        | mitre                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                               |
| Published       | 2016-04-07 19:59:04 UTC                                                                                                    |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                    |
| Description     | The chat feature in the Real-Time Collaboration (RTC) services 7.3 and 7.4 in SAP NetWeaver Java AS 7.1 through 7.5 all... |

## Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov | Primary | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 2.0     | nvd@nist.gov | Primary | 5     |          | AV:N/AC:L/Au:N/C:P/I:N/A:N                   |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                           | Version | Update | Edition | Language |
|-------------|--------|-----------------------------------|---------|--------|---------|----------|
| Application | Sap    | Netweaver Application Server Java | All     | All    | All     | All      |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

## References

| Reference                                                                                              | Source                    |
|--------------------------------------------------------------------------------------------------------|---------------------------|
| SAP NetWeaver AS JAVA 7.5 Information Disclosure ≈ Packet Storm                                        | af854a3a-2127-422b-91ae-5 |
| [ERPSCAN-16-016] SAP NetWeaver Java AS WD_CHAT - Information disclosure vulnerability                  | af854a3a-2127-422b-91ae-5 |
| Full Disclosure: [ERPSCAN-16-016] SAP NetWeaver Java AS WD_CHAT - Information disclosure vulnerability | af854a3a-2127-422b-91ae-5 |
| SAP Security Notes March 2016 - Review                                                                 | af854a3a-2127-422b-91ae-5 |
| CVE Program record                                                                                     | CVE.ORG                   |
| NVD vulnerability detail                                                                               | NVD                       |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)