



CVE-2017-15708

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-15708 |
| State | PUBLIC |
| Assigner | security@apache.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-12-11 15:29:00 UTC |
| Updated | 2023-11-07 02:40:00 UTC |
| Description | In Apache Synapse, by default no authentication is required for Java Remote Method Invocation (RMI). So Apache Synaps |

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|-------------------------------------|---------|--------|---------|----------|
| Application | Apache | Commons Collections | All | All | All | All |
| Application | Apache | Synapse | 1.0 | All | All | All |
| Application | Apache | Synapse | 1.1 | All | All | All |
| Application | Apache | Synapse | 1.1.1 | All | All | All |
| Application | Apache | Synapse | 1.1.2 | All | All | All |
| Application | Apache | Synapse | 1.2 | All | All | All |
| Application | Apache | Synapse | 2.0.0 | All | All | All |
| Application | Apache | Synapse | 2.1.0 | All | All | All |
| Application | Apache | Synapse | 3.0.0 | All | All | All |
| Application | Apache | Synapse | 1.0 | All | All | All |
| Application | Apache | Synapse | 1.1 | All | All | All |
| Application | Apache | Synapse | 1.1.1 | All | All | All |
| Application | Apache | Synapse | 1.1.2 | All | All | All |
| Application | Apache | Synapse | 1.2 | All | All | All |
| Application | Apache | Synapse | 2.0.0 | All | All | All |
| Application | Apache | Synapse | 2.1.0 | All | All | All |
| Application | Apache | Synapse | 3.0.0 | All | All | All |

| | | | | | | |
|-------------|------------------------|---|-------|-----|-----|-----|
| Application | Oracle | Financial Services Market Risk Measurement And Management | 8.0.6 | All | All | All |
| Application | Oracle | Financial Services Market Risk Measurement And Management | 8.0.8 | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.56 | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.57 | All | All | All |

References

Reference

[Apache Commons Collections: Remote code execution \(GLSA 202107-37\) — Gentoo security](#)

[Oracle Critical Patch Update Advisory - July 2020](#)

[Multiple Apache Products CVE-2017-15708 Remote Code Execution Vulnerability](#)

[\[doris-commits\] 20210402 \[GitHub\] \[incubator-doris\] zh0122 opened a new pull request #5595: \[FE\]\[Fix\]Update commons-collections to fix a s](#)

[Pony Mail!](#)

[Oracle Critical Patch Update Advisory - January 2020](#)

[Pony Mail!](#)

[Pony Mail!](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710031](#) [Gentoo Linux Apache Commons Collections Remote code execution \(GLSA 202107-37\)](#)

[92029](#) [Microsoft SQL Server Multiple Vulnerabilities](#)

[982335](#) [Java \(maven\) Security Update for org.apache.synapse:synapse-core \(GHSA-p694-23q3-rvrc\)](#)

© [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](#).

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