



CVE-2018-2492

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

Summary

CVE	CVE-2018-2492
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-11 22:29:00 UTC
Updated	2021-04-20 19:21:00 UTC
Description	SAML 2.0 functionality in SAP NetWeaver AS Java, does not sufficiently validate XML documents received from an untrusted

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	7.20	All	All	All
Application	Sap	Netweaver	7.30	All	All	All
Application	Sap	Netweaver	7.31	All	All	All
Application	Sap	Netweaver	7.40	All	All	All
Application	Sap	Netweaver	7.50	All	All	All
Application	Sap	Netweaver	7.20	All	All	All
Application	Sap	Netweaver	7.30	All	All	All
Application	Sap	Netweaver	7.31	All	All	All
Application	Sap	Netweaver	7.40	All	All	All
Application	Sap	Netweaver	7.50	All	All	All
Application	Sap	Netweaver Application Server Java	7.20	All	All	All
Application	Sap	Netweaver Application Server Java	7.30	All	All	All
Application	Sap	Netweaver Application Server Java	7.31	All	All	All
Application	Sap	Netweaver Application Server Java	7.40	All	All	All
Application	Sap	Netweaver Application Server Java	7.50	All	All	All

References

Reference	Source	Link	Tag
launchpad.support.sap.com	MISC	launchpad.support.sap.com	Per
SAP NetWeaver AS Java CVE-2018-2492 XML External Entity Injection Vulnerability	BID	www.securityfocus.com	Thi
SAP Security Patch Day – December 2018 - Product Security Response at SAP - SCN Wiki	MISC	wiki.scn.sap.com	Ver
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report