



CVE-2022-41271

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

Summary

CVE	CVE-2022-41271
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-13 03:15:00 UTC
Updated	2023-11-07 03:52:00 UTC
Description	An unauthenticated user can attach to an open interface exposed through JNDI by the Messaging System of SAP NetWeaver

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Process Integration	7.50	All	All	All

References

Reference	Source	Link	Tags
Access Denied	MISC	www.sap.com	
launchpad.support.sap.com	MISC	launchpad.support.sap.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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