



CVE-2014-0995

Published on: 11/06/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:56 PM UTC

CVE-2014-0995

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Netweaver](#) from [Sap](#) contain the following vulnerability:

The Standalone Enqueue Server in SAP Netweaver 7.20, 7.01, and earlier allows remote attackers to cause a denial of service (uncontrolled recursion and crash) via a trace level with a wildcard in the Trace Pattern.

CVE-2014-0995 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

JavaScript is not available.

[Broken Link](#)
[nitter.domain.glass](#)
[text/html](#)

[CONFIRM](#)
twitter.com/SAP_Gsupport/status/522750365780160513

IBM X-Force Exchange

[Third Party Advisory](#)
[VDB Entry](#)
exchange.xforce.ibmcloud.com
[text/html](#)

[XF netweaver-trace-pattern-dos\(97610\)](#)

Full Disclosure: [CORE-2014-0007] -SAP
Netweaver Enqueue Server Trace Pattern Denial
of Service Vulnerability

[Exploit](#)
[Mailing List](#)
[Third Party Advisory](#)
[seclists.org](#)
[text/html](#)

[FULLDISC 20141016 \[CORE-2014-0007\] -SAP
Netweaver Enqueue Server Trace Pattern Denial of
Service Vulnerability](#)

SAP Netweaver Enqueue Server Trace Pattern
Denial Of Service Packet Storm

[Exploit](#)
[Third Party Advisory](#)

[packetstormsecurity.com/files/128726/SAP-
Netweaver-Enqueue-Server-Trace-Pattern-Denial-Of-
Service-Vulnerability](https://packetstormsecurity.com/files/128726/SAP-Netweaver-Enqueue-Server-Trace-Pattern-Denial-Of-Service-Vulnerability)

Denial of Service - Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	Netweaver Enqueue Server Trace Pattern Denial of Service.html
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/x-python	BUGTRAQ 20141016 [CORE-2014-0007] -SAP Netweaver Enqueue Server Trace Pattern Denial of Service Vulnerability
Analyzing SAP Security Notes October 2014 Edition Onapsis	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC blog.onapsis.com/analyzing-sap-security-notes-october-2014-edition/
Security Advisory SA60950 - SAP Netweaver Enqueue Server Packet Handling Denial of Service Vulnerability - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 60950
SAP Netweaver Enqueue Server Trace Pattern Denial of Service Vulnerability - CoreLabs Advisory	Exploit Third Party Advisory www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/sap-netweaver-enqueue-server-trace-pattern-denial-service-vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	7.20	All	All	All
Application	Sap	Netweaver	7.20	All	All	All
Application	Sap	Netweaver	All	All	All	All
cpe:2.3:a:sap:netweaver:7.20:*****:..						
cpe:2.3:a:sap:netweaver:7.20:*****:..						
cpe:2.3:a:sap:netweaver:*****:..						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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