



CVE-2012-2511

Published on: 05/14/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:25 PM UTC

CVE-2012-2511

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The DiagTraceAtoms function in disp+work.exe 7010.29.15.58313 and 7200.70.18.23869 in the Dispatcher in SAP NetWeaver 7.0 EHP1 and EHP2 allows remote attackers to cause a denial of service (daemon crash) via a crafted SAP Diag packet.

CVE-2012-2511 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

No Description Provided

Tags

[service.sap.com](#)
[text/html](#)

Link

[MISC](#)
[service.sap.com/sap/support/notes/1687910](#)

Acknowledgments to Security Researchers | SCN

[scn.sap.com](#)
[text/html](#)

[CONFIRM](#) [scn.sap.com/docs/DOC-8218](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF netweaver-diagtraceatoms-dos\(75453\)](#)

SAP NetWeaver Dispatcher Bugs Let Remote Users Execute Arbitrary Code and Deny Service - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1027052](#)

Core Security Technologies

[Exploit](#)
[www.coresecurity.com](#)
[text/html](#)

[MISC](#)
[www.coresecurity.com/content/sap-netweaver-dispatcher-multiple-vulnerabilities](#)

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	7.0	ehp1	All	All
Application	Sap	Netweaver	7.0	ehp2	All	All
Application	Sap	Netweaver	7.0	ehp1	All	All
Application	Sap	Netweaver	7.0	ehp2	All	All
cpe:2.3:a:sap:netweaver:7.0:ehp1:*****:						
cpe:2.3:a:sap:netweaver:7.0:ehp2:*****:						
cpe:2.3:a:sap:netweaver:7.0:ehp1:*****:						
cpe:2.3:a:sap:netweaver:7.0:ehp2:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)