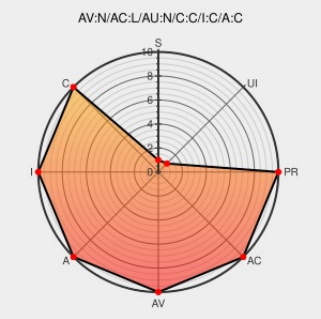
CVE-2012-4341

Published on: 08/15/2012 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:11:00 AM UTC

CVE-2012-4341

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Netweaver Abap from Sap contain the following vulnerability:

Multiple stack-based buffer overflows in msg_server.exe in SAP NetWeaver ABAP 7.x allow remote attackers to cause a denial of service (crash) and execute arbitrary code via a (1) long parameter value, (2) crafted string size field, or (3) long Parameter Name string in a package with opcode 0x43 and sub opcode 0x4 to TCP port 3900.

CVE-2012-4341 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SAP NetWeaver ABAP Flaw in 'msg_server.exe' Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1027211
Acknowledgments to Security Researchers | SCN	scn.sap.com text/html	CONFIRM scn.sap.com/docs/DOC-8218
Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-12-104/
Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-12-111/
Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-12-112/

Security Advisory SA49744 - SAP NetWeaver Multiple Buffer Overflow Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 49744
No Description Provided	service.sap.com text/html	MISC service.sap.com/sap/support/notes/1649838
SAP Service Marketplace has been retired	websmp230.sap-ag.de text/html	MISC websmp230.sap-ag.de/sap(bD1lbiZjPTAwMQ==)/bc/bsp/spn/sapnotes/index2.htm?numm=1649840

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 Abap	7.0	All	All	All
Application	Sap	Netweaver Abap	7.02	sp6	All	All
Application	Sap	Netweaver Abap	7.03	sp4	All	All
Application	Sap	Netweaver Abap	7.0	All	All	All
Application	Sap	Netweaver Abap	7.02	sp6	All	All
Application	Sap	Netweaver Abap	7.03	sp4	All	All

cpe:2.3:a:sap:netweaver_abap:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.02:sp6:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.03:sp4:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.02:sp6:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.03:sp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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