

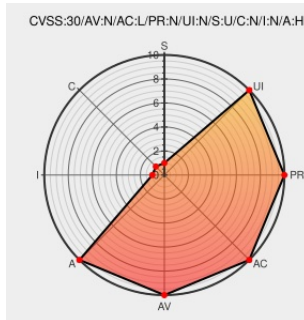


CVE-2021-27628

Published on: 06/09/2021 12:00:00 AM UTC

Last Modified on: 10/31/2022 02:46:00 PM UTC

CVE-2021-27628

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

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

SAP NetWeaver ABAP Server and ABAP Platform (Dispatcher), versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an

unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method DpRTmPrepareReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.

CVE-2021-27628 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
SAP Security Patch Day – June 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	 MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=578125999
Full Disclosure: Onapsis Security Advisory 2021-0015: [Multiple CVEs] Memory Corruption vulnerability in SAP NetWeaver ABAP Dispatcher service	seclists.org text/html	 FULLDISC 20211022 Onapsis Security Advisory 2021-0015: [Multiple CVEs] Memory Corruption vulnerability in SAP NetWeaver ABAP Dispatcher service
No Description Provided	launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/3021197
SAP NetWeaver ABAP Dispatcher Service Memory Corruption ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/164591/SAP-NetWeaver-ABAP-Dispatcher-Service-Memory-Corruption.html

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver As Abap	kernel_7.22	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.49	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.53	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.73	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.77	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.81	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.82	All	All	All
Application	Sap	Netweaver As Abap	kernel_7.83	All	All	All
Application	Sap	Netweaver As Abap	kernel_8.04	All	All	All
Application	Sap	Netweaver As Abap	krnl32nuc_7.22	All	All	All
Application	Sap	Netweaver As Abap	krnl32nuc_7.22ext	All	All	All
Application	Sap	Netweaver As Abap	krnl32uc_7.22	All	All	All
Application	Sap	Netweaver As Abap	krnl32uc_7.22ext	All	All	All
Application	Sap	Netweaver As Abap	krnl64nuc_7.22	All	All	All

Application	Sap	Netweaver As Abap	krnl64nuc_7.22	All	All	All
Application	Sap	Netweaver As Abap	krnl64nuc_7.22ext	All	All	All
Application	Sap	Netweaver As Abap	krnl64nuc_7.49	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_7.22	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_7.22ext	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_7.49	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_7.53	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_7.73	All	All	All
Application	Sap	Netweaver As Abap	krnl64uc_8.04	All	All	All
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.22:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.49:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.53:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.73:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.77:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.81:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.82:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_7.83:*****:						
cpe:2.3:a:sap:netweaver_as_abap:kernel_8.04:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl32nuc_7.22:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl32nuc_7.22ext:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl32uc_7.22:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl32uc_7.22ext:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_7.22:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_7.22ext:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_7.49:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_7.22:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_7.22ext:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_7.49:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_7.53:*****:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_7.73:*****:						
cpe:2.3:a:sap:netweaver as abap:krnl64uc_8.04:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-27628 : #SAP NetWeaver ABAP Server and ABAP Platform Dispatcher , versions - KRNL32NUC - 7.22,7.22EXT, KR... twitter.com/i/web/status/1...	2021-06-09 14:07:13

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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