



# CVE-2022-22543

Published on: 02/09/2022 12:00:00 AM UTC

Last Modified on: 10/25/2022 08:39:00 PM UTC

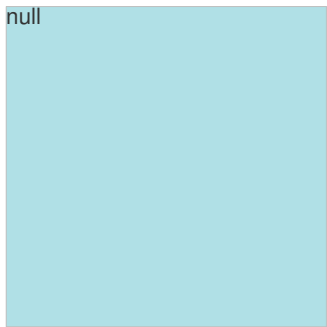
## CVE-2022-22543

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel) - versions KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, does not sufficiently validate sap-passport information, which could lead to a Denial-of-Service attack.

This allows an unauthorized remote user to provoke a breakdown of the SAP Web Dispatcher or Kernel work process. The crashed process can be restarted immediately, other processes are not affected.

CVE-2022-22543 has been assigned by [sap](#) [cna@sap.com](mailto: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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>NONE</b>	<b>HIGH</b>

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>NONE</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
-------------	------	------

SAP Security Patch Day - February 2022 - Product Security Response at SAP - Community Wiki

wiki.scn.sap.com  
text/html

MISC  
wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day++February+2022

No Description Provided

launchpad.support.sap.com  
text/html

MISC launchpad.support.sap.com/#/notes/3116223

SAP Patch Day Blog

web.archive.org  
text/html  
Inactive Link Not Archived

MISC www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.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](mailto: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	7.22	All	All	All
Application	Sap	Netweaver Abap	7.22ext	All	All	All
Application	Sap	Netweaver Abap	7.49	All	All	All
Application	Sap	Netweaver Abap	7.53	All	All	All
Application	Sap	Netweaver Abap	7.77	All	All	All
Application	Sap	Netweaver Abap	7.81	All	All	All
Application	Sap	Netweaver Abap	7.85	All	All	All
Application	Sap	Netweaver Abap	7.86	All	All	All
Application	Sap	Netweaver Abap	7.87	All	All	All
Application	Sap	Netweaver Abap	8.04	All	All	All
Application	Sap	Netweaver Abap	krnl64nuc_7.22	All	All	All
Application	Sap	Netweaver Abap	krnl64nuc_8.04	All	All	All
Application	Sap	Netweaver As Abap	7.22	All	All	All
Application	Sap	Netweaver As Abap	7.22ext	All	All	All
Application	Sap	Netweaver As Abap	7.49	All	All	All
Application	Sap	Netweaver As Abap	7.53	All	All	All
Application	Sap	Netweaver As Abap	7.77	All	All	All
Application	Sap	Netweaver As Abap	7.81	All	All	All
Application	Sap	Netweaver As Abap	7.85	All	All	All
Application	Sap	Netweaver As Abap	7.86	All	All	All
Application	Sap	Netweaver As Abap	7.87	All	All	All
Application	Sap	Netweaver As Abap	8.04	All	All	All

Application	Sap	Netweaver As Abap	0.04	All	All	All
Application	Sap	Netweaver As Abap	krnl64nuc_7.22	All	All	All
Application	Sap	Netweaver As Abap	krnl64nuc_8.04	All	All	All
cpe:2.3:a:sap:netweaver_abap:7.22:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.22ext:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.49:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.53:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.77:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.81:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.85:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.86:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:7.87:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:8.04:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:krnl64nuc_7.22:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_abap:krnl64nuc_8.04:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.22:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.22ext:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.49:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.53:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.77:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.81:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.85:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.86:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:7.87:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:8.04:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_7.22:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_8.04:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Social mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-22543 : #SAP NetWeaver Application Server for ABAP Kernel and ABAP Platform Kernel - versions KERNEL 7... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-02-09 23:25:09

[← 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](https://status.cve.report)**