



# CVE-2021-38162

Published on: 09/14/2021 12:00:00 AM UTC

Last Modified on: 05/05/2022 12:15:00 AM UTC

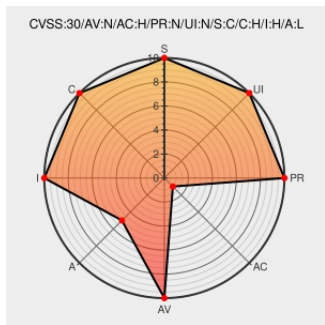
## CVE-2021-38162

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SAP Web Dispatcher versions - 7.49, 7.53, 7.77, 7.81, KRNL64NUC - 7.22, 7.22EXT, 7.49, KRNL64UC -7.22, 7.22EXT, 7.49, 7.53, KERNEL - 7.22, 7.49, 7.53, 7.77, 7.81, 7.83 processes allow an unauthenticated attacker to submit a malicious crafted request over a network to a front-end server which may, over several attempts, result in a back-end server confusing the boundaries of malicious and legitimate messages. This can result in the back-end server executing a malicious payload which can be used to read or modify any information on the server or consume server resources making it temporarily unavailable.

CVE-2021-38162 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.4 - CRITICAL**

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>HIGH</b>	<b>HIGH</b>	<b>LOW</b>

CVSS2 Score: **7.5 - HIGH**


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

## CVE References

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

Full Disclosure: Onapsis Security Advisory 2022-0001: HTTP Request Smuggling in SAP Web Dispatcher

[seclists.org](https://seclists.org)  
text/html

 FULLDISC 20220504 Onapsis Security Advisory 2022-0001: HTTP Request Smuggling in SAP Web Dispatcher

SAP Security Patch Day – September 2021 - Product Security Response at SAP - Community Wiki

[wiki.scn.sap.com](https://wiki.scn.sap.com)  
text/html

 MISC  
[wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405](https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405)


No Description Provided

[launchpad.support.sap.com](https://launchpad.support.sap.com)  
text/html

 MISC  
[launchpad.support.sap.com/#/notes/3080567](https://launchpad.support.sap.com/#/notes/3080567)

SAP Web Dispatcher HTTP Request Smuggling ~ Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com)  
text/html

 MISC  
[packetstormsecurity.com/files/166964/SAP-Web-Dispatcher-HTTP-Request-Smuggling.html](https://packetstormsecurity.com/files/166964/SAP-Web-Dispatcher-HTTP-Request-Smuggling.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	Web Dispatcher	7.22ext	All	All	All
Application	Sap	Web Dispatcher	7.49	All	All	All
Application	Sap	Web Dispatcher	7.53	All	All	All
Application	Sap	Web Dispatcher	7.77	All	All	All
Application	Sap	Web Dispatcher	7.81	All	All	All
Application	Sap	Web Dispatcher	7.83	All	All	All
Application	Sap	Web Dispatcher	kernel_7.22	All	All	All
Application	Sap	Web Dispatcher	krnl64nuc_7.22	All	All	All
Application	Sap	Web Dispatcher	krnl64uc_7.22	All	All	All

cpe:2.3:a:sap:web\_dispatcher:7.22ext:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:7.49:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:7.53:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:7.77:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:7.81:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:7.83:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:kernel\_7.22:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:krnl64nuc\_7.22:\*:\*:\*:\*:\*:

cpe:2.3:a:sap:web\_dispatcher:krnl64uc\_7.22:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-38162 : #SAP Web Dispatcher versions - 7.49, 7.53, 7.77, 7.81, KRNL64NUC - 7.22, 7.22EXT, 7.49, KRNL64UC -... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-14 12:10:33

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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)