

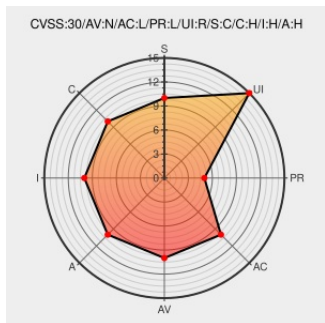


CVE-2020-6284

Published on: 08/12/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:04 PM UTC

CVE-2020-6284

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

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

SAP NetWeaver (Knowledge Management), versions - 7.30, 7.31, 7.40, 7.50, allows the automatic execution of script content in a stored file due to inadequate filtering with the accessing user's privileges. If the accessing user has administrative privileges, then the execution of the script content could result in complete compromise of system confidentiality, integrity and availability, leading to Stored Cross Site Scripting.

CVE-2020-6284 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [sap](#) **SAP SE - SAP NetWeaver (Knowledge Management)** version **7.30**

Affected Vendor/Software: [sap](#) **SAP SE - SAP NetWeaver (Knowledge Management)** version **7.31**

Affected Vendor/Software: [sap](#) **SAP SE - SAP NetWeaver (Knowledge Management)** version **7.40**

Affected Vendor/Software: [sap](#) **SAP SE - SAP NetWeaver (Knowledge Management)** version **7.50**

CVSS3 Score: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

CVE References

Description	Tags	Link
No Description Provided	Permissions Required launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#!/notes/2928635
SAP Security Patch Day – August 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	 MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552603345

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.

Related QID Numbers

87459 SAP NetWeaver AS Java Remote Code Execution Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Knowledge Management	7.30	All	All	All
Application	Sap	Netweaver Knowledge Management	7.31	All	All	All
Application	Sap	Netweaver Knowledge Management	7.40	All	All	All
Application	Sap	Netweaver Knowledge Management	7.50	All	All	All
Application	Sap	Netweaver Knowledge Management	7.30	All	All	All
Application	Sap	Netweaver Knowledge Management	7.31	All	All	All
Application	Sap	Netweaver Knowledge Management	7.40	All	All	All
Application	Sap	Netweaver Knowledge Management	7.50	All	All	All
cpe:2.3:a:sap:netweaver_knowledge_management:7.30:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.31:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.40:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.50:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.30:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.31:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.40:*****:						
cpe:2.3:a:sap:netweaver_knowledge_management:7.50:*****:						

No vendor comments have been submitted for this CVE

← 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](#)