



CVE-2021-37531

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

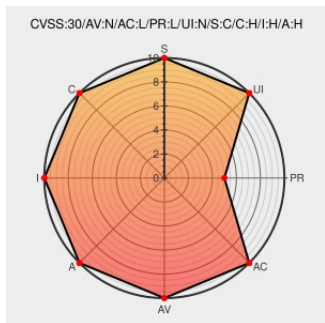
Last Modified on: 09/24/2021 08:17:00 PM UTC

CVE-2021-37531

Source: Mitre

Source: Nist

Print: PDF



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

SAP NetWeaver Knowledge Management XML Forms versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, contains an XSLT vulnerability which allows a non-administrative authenticated attacker to craft a malicious XSL stylesheet file containing a script with OS-level commands, copy it into a location to be accessed by the system and then create a file

which will trigger the XSLT engine to execute the script contained within the malicious XSL file. This can result in a full compromise of the confidentiality, integrity, and availability of the system.

CVE-2021-37531 has been assigned by [cna@sap.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

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

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

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

 MISC
wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405

No Description Provided

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

 MISC
launchpad.support.sap.com/#/notes/3081888

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 Knowledge Management Xml Forms	7.10	All	All	All
Application	Sap	Netweaver Knowledge Management Xml Forms	7.11	All	All	All
Application	Sap	Netweaver Knowledge Management Xml Forms	7.30	All	All	All
Application	Sap	Netweaver Knowledge Management Xml Forms	7.31	All	All	All
Application	Sap	Netweaver Knowledge Management Xml Forms	7.40	All	All	All
Application	Sap	Netweaver Knowledge Management Xml Forms	7.50	All	All	All

`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.10:***:***:***:`

`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.11:***:***:***:`

`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.30:***:***:***:`


`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.31:***:***:***:`

`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.40:***:***:***:`

`cpe:2.3:a:sap:netweaver_knowledge_management_xml_forms:7.50:***:***:***:`

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37531 : #SAP NetWeaver Knowledge Management XML Forms versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, conta... twitter.com/i/web/status/1...	2021-09-14 12:09:12

[← Previous ID](#)

[Next ID →](#)

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](#)