



CVE-2021-21475

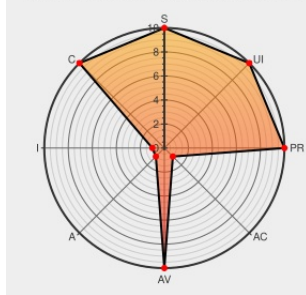
Published on: 02/09/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:59 PM UTC

CVE-2021-21475

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

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N



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

Under specific circumstances SAP Master Data Management, versions - 710, 710.750, allows an unauthorized attacker to exploit insufficient validation of path information provided by users, thus characters representing 'traverse to parent directory' are passed through to the file APIs. Due to this Directory Traversal vulnerability the attacker could read content of arbitrary files on the remote server and expose sensitive data.

CVE-2021-21475 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Master Data Management Server** version **710**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Master Data Management Server** version **710.750**

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	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link				
No Description Provided	Permissions Required launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/3000897				
SAP Security Patch Day – February 2021 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	 MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=568460543				
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 Master Data Management Server	710	All	All	All
Application	Sap	Netweaver Master Data Management Server	710.750	All	All	All
Application	Sap	Netweaver Master Data Management Server	710	All	All	All
Application	Sap	Netweaver Master Data Management Server	710.750	All	All	All
cpe:2.3:a:sap:netweaver_master_data_management_server:710:*****:.*						
cpe:2.3:a:sap:netweaver_master_data_management_server:710.750:*****:.*						
cpe:2.3:a:sap:netweaver_master_data_management_server:710:*****:.*						
cpe:2.3:a:sap:netweaver_master_data_management_server:710.750:*****:.*						
No vendor comments have been submitted for this CVE						
← Previous ID		Next ID →				