

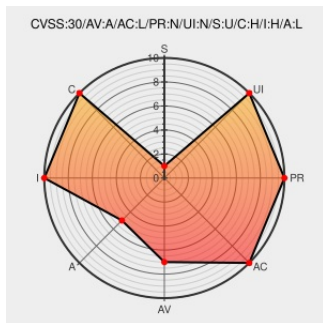


CVE-2021-21482

Published on: 04/13/2021 12:00:00 AM UTC

Last Modified on: 06/28/2022 02:11:00 PM UTC

CVE-2021-21482

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

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

SAP NetWeaver Master Data Management, versions - 710, 710.750, allows a malicious unauthorized user with access to the MDM Server subnet to find the password using a brute force method. If successful, the attacker could obtain access to highly sensitive data and MDM administrative privileges leading to information disclosure vulnerability

thereby affecting the confidentiality and integrity of the application. This happens when security guidelines and recommendations concerning administrative accounts of an SAP NetWeaver Master Data Management installation have not been thoroughly reviewed.

CVE-2021-21482 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** version **710**

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

CVSS3 Score: **8.3 - HIGH**

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

CVSS2 Score: **4.8 - MEDIUM**

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

CVE References

Description

Tags

Link

No Description Provided

[launchpad.support.sap.com](https://launchpad.support.sap.com/#/notes/3017908)
[text/html](#)

 MISC
launchpad.support.sap.com/#/notes/3017908

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

[wiki.scn.sap.com](https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649)
[text/html](#)

 MISC
wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

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	7.10.750	All	All	All
Application	Sap	Netweaver Master Data Management	710	All	All	All
<code>cpe:2.3:a:sap:netweaver_master_data_management:7.10.750:*:*:*:*:*:</code>						
<code>cpe:2.3:a:sap:netweaver_master_data_management:710:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← 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](#)