

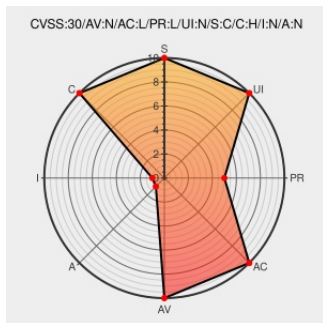


CVE-2020-6249

Published on: 05/12/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:05 PM UTC

CVE-2020-6249

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

Certain versions of [Master Data Governance S4core](#) from [Sap](#) contain the following vulnerability:

The use of an admin backend report within SAP Master Data Governance, versions - S4CORE 101, S4FND 102, 103, 104, SAP_BS_FND 748; allows an attacker to execute crafted database queries, exposing the backend database, leading to SQL Injection.

CVE-2020-6249 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Master Data Governance (S4CORE) version 101**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Master Data Governance (S4FND) version 102**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Master Data Governance (S4FND) version 103**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Master Data Governance (S4FND) version 104**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Master Data Governance (SAP_BS_FND) version 748**

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: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
SAP Security Patch Day – May 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	SAP MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=545396222
No Description Provided	Permissions Required launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#/notes/2908560

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	Master Data Governance S4core	101	All	All	All
Application	Sap	Master Data Governance S4core	101	All	All	All
Application	Sap	Master Data Governance S4fnd	102	All	All	All
Application	Sap	Master Data Governance S4fnd	103	All	All	All
Application	Sap	Master Data Governance S4fnd	104	All	All	All
Application	Sap	Master Data Governance S4fnd	102	All	All	All
Application	Sap	Master Data Governance S4fnd	103	All	All	All
Application	Sap	Master Data Governance S4fnd	104	All	All	All
Application	Sap	Master Data Governance Sap Bs Fnd	748	All	All	All
Application	Sap	Master Data Governance Sap Bs Fnd	748	All	All	All

cpe:2.3:a:sap:master_data_governance_(s4core):101:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4core):101:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):102:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):103:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):104:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):102:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):103:*****:.*:

cpe:2.3:a:sap:master_data_governance_(s4fnd):104:*****:.*:

cpe:2.3:a:sap:master_data_governance_(sap_bs_fnd):748.*.*.*.*.*.*.*.*.*.*

cpe:2.3:a:sap:master_data_governance_(sap_bs_fnd):748.*.*.*.*.*.*.*.*.*.*

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](#)