



CVE-2020-6210

Published on: 03/10/2020 12:00:00 AM UTC

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

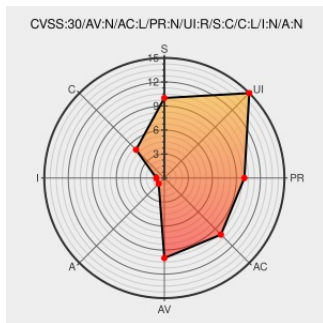
CVE-2020-6210

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Fiori Launchpad](#) from [Sap](#) contain the following vulnerability:

SAP Fiori Launchpad, versions- 753, 754, does not sufficiently encode user-controlled inputs, and hence allowing the attacker to inject the meta tag into the launchpad html using the vulnerable parameter, leading to reflected Cross-Site Scripting (XSS) vulnerability.

CVE-2020-6210 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [sap](#) **SAP SE - SAP Fiori Launchpad** version **753**

Affected Vendor/Software: [sap](#) **SAP SE - SAP Fiori Launchpad** version **754**

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link

No Description Provided

Permissions Required

launchpad.support.sap.com

text/html

SAP MISC

launchpad.support.sap.com/#/notes/2864462

SAP Security Patch Day – March 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?pagelId=540935305

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	Fiori Launchpad	753	All	All	All
Application	Sap	Fiori Launchpad	754	All	All	All
Application	Sap	Fiori Launchpad	753	All	All	All
Application	Sap	Fiori Launchpad	754	All	All	All

cpe:2.3:a:sap:fiori_launchpad:753:*****:*

cpe:2.3:a:sap:fiori_launchpad:754:*****:*

cpe:2.3:a:sap:fiori_launchpad:753:*****:*

cpe:2.3:a:sap:fiori_launchpad:754:*****:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→