



CVE-2020-1949

Published on: 04/01/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:47 PM UTC

CVE-2020-1949

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

Certain versions of [Sling Cms](#) from [Apache](#) contain the following vulnerability:

Scripts in Sling CMS before 0.16.0 do not properly escape the Sling Selector from URLs when generating navigational elements for the administrative consoles and are vulnerable to reflected XSS attacks.

CVE-2020-1949 has been assigned by [security@apache.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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
CVE-2020-1949: Apache Sling CMS Reflected XSS Vulnerability	Mailing List Vendor Advisory s.apache.org text/xml	MISC s.apache.org/CVE-2020-1949

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	Apache	Sling Cms	All	All	All	All
Application	Apache	Sling Cms	All	All	All	All
cpe:2.3:a:apache:sling_cms:*****:.*						
cpe:2.3:a:apache:sling_cms:*****:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)