

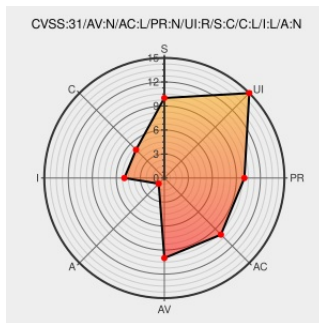


CVE-2018-25052

Published on: Not Yet Published

Last Modified on: 01/06/2023 07:11:00 PM UTC

CVE-2018-25052

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

Certain versions of [Catalyst-plugin-session](#) from [Catalyst-plugin-session Project](#) contain the following vulnerability:

A vulnerability has been found in Catalyst-Plugin-Session up to 0.40 and classified as problematic. This vulnerability affects the function `_load_sessionid` of the file `lib/Catalyst/Plugin/Session.pm` of the component Session ID Handler. The manipulation of the argument `sid` leads to cross site scripting. The attack can be initiated remotely.

Upgrading to version 0.41 is able to address this issue. The name of the patch is `88d1b599e1163761c9bd53bec53ba078f13e09d4`. It is recommended to upgrade the affected component. VDB-216958 is the identifier assigned to this vulnerability.

CVE-2018-25052 has been assigned by [cna@vuldb.com](#) 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

CVE References

Description	Tags	Link
Session: encode HTML entities in error · perl-catalyst/Catalyst-Plugin-Session@88d1b59 · GitHub	github.com text/html	MISC github.com/perl-catalyst/Catalyst-Plugin-Session/commit/88d1b599e1163761c9bd53bec53ba078f13e09d4
CVE-2018-25052 Catalyst-Plugin-Session Session ID Session.pm _load_sessionid cross site scripting	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.216958
CVE-2018-25052 Catalyst-Plugin-Session Session ID Session.pm _load_sessionid cross site scripting	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.216958

Cross Site Scripting

Inactive LinkNot Archived

Release 0.41 · perl-catalyst/Catalyst-Plugin-Session · GitHub

github.comtext/html

MISC github.com/perl-catalyst/Catalyst-Plugin-Session/releases/tag/0.41

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	Catalyst-plugin-session Project	Catalyst-plugin-session	All	All	All	All

cpe:2.3:a:catalyst-plugin-session_project:catalyst-plugin-session:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →