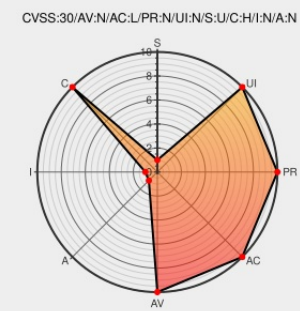
CVE-2017-16248

Published on: 10/31/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16248

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Catalyst-plugin-static-simple from Catalyst-plugin-static-simple Project contain the following vulnerability:

The Catalyst-Plugin-Static-Simple module before 0.34 for Perl allows remote attackers to read arbitrary files if there is a '.' character anywhere in the pathname, which differs from the intended policy of allowing access only when the filename itself has a '.' character.

CVE-2017-16248 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Changes - metacpan.org	Release Notes, metacpan.org, text/html	CONFIRM metacpan.org/changes/distribution/Catalyst-Plugin-Static-Simple
#880458 - libcatalyst-plugin-static-simple-perl: CVE-2017-16248: leaks	Third Party Advisory	CONFIRM bugs.debian.org/880458

files without extention, inadvertently - Debian Bug report logs	bugs.debian.org text/html	
Bug #120558 for Catalyst-Plugin-Static-Simple: Will inadvertantly serve any file if a directory in the path has a dot (.)	Issue Tracking Third Party Advisory rt.cpan.org text/html	CONFIRM rt.cpan.org/Public/Bug/Display.html?id=120558

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-static-simple Project	Catalyst-plugin-static-simple	All	All	All	All
Application	Catalyst-plugin-static-simple Project	Catalyst-plugin-static-simple	All	All	All	All

cpe:2.3:a:catalyst-plugin-static-simple_project:catalyst-plugin-static-simple:*:*:*:*:*:perl:*:*:

cpe:2.3:a:catalyst-plugin-static-simple_project:catalyst-plugin-static-simple:*:*:*:*:*:perl:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→