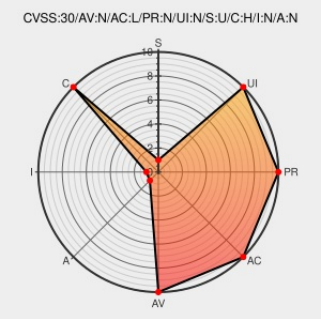
CVE-2018-17605

Published on: 09/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:19 PM UTC

CVE-2018-17605

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



Certain versions of Asset-pipeline from Asset Pipeline Project contain the following vulnerability:

An issue was discovered in the Asset Pipeline plugin before 3.0.4 for Grails. An attacker can perform directory traversal via a crafted request when a servlet-based application is executed in Jetty, because there is a classloader vulnerability that can allow a reverse file traversal route in AssetPipelineFilter.groovy or AssetPipelineFilterCore.groovy.

CVE-2018-17605 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
fixing jetty classloader vulnerability with potential reverse file tr… · bertramdev/asset-pipeline@a29533c · GitHub	Patch, github.com, text/html	MISC github.com/bertramdev/asset-pipeline/commit/a29533c52e4b60e244082433e116d2a038d01017

File reading vulnerability · Issue #11068 · grails/grails-core · GitHub

Third Party Advisory
github.com
text/html

MISC github.com/grails/grails-core/issues/11068

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asset Pipeline Project	Asset-pipeline	All	All	All	All
Application	Asset Pipeline Project	Asset-pipeline	All	All	All	All

cpe:2.3:a:asset_pipeline_project:asset-pipeline:*:*:*:*:*:grails:*:*

cpe:2.3:a:asset_pipeline_project:asset-pipeline:*:*:*:*:*:grails:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→