



CVE-2018-1000817

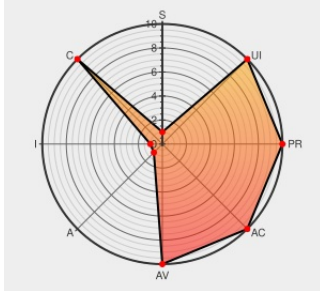
Published on: 12/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000817

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Asset-pipeline](#) from [Asset Pipeline Project](#) contain the following vulnerability:

Asset Pipeline Grails Plugin Asset-pipeline plugin version Prior to 2.14.1.1, 2.15.1 and 3.0.6 contains a Incorrect Access Control vulnerability in Applications deployed in Jetty that can result in Download .class files and any arbitrary file. This attack appear to be exploitable via Specially crafted GET request containing directory traversal from assets-pipeline context. This vulnerability appears to have been fixed in 2.14.1.1 (for Grails 2.x), 2.15.1 (for Grails 3 and Java 7) and 3.0.6 (for Grails 3 and Java 8).

CVE-2018-1000817 has been assigned by [M](#) 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
Redirection	CVE-2018-1000817	MICO

Redirecting...

Exploit

Third Party Advisory

grailsblog.objectcomputing.com

text/html

MISC

grailsblog.objectcomputing.com/posts/2018/09/23/security-vulnerability-in-asset-pipeline-and-jetty.html

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

Third Party Advisory

github.com

text/html

MISC

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

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	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 →