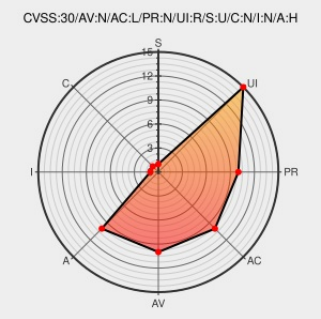
CVE-2018-17292

Published on: 09/21/2018 12:00:00 AM UTC

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

CVE-2018-17292

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



Certain versions of Webassembly Virtual Machine from Webassembly Virtual Machine Project contain the following vulnerability:

An issue was discovered in WAVM before 2018-09-16. The loadModule function in Include/Inline/CLI.h lacks checking of the file length before a file magic comparison, allowing attackers to cause a Denial of Service (application crash caused by out-of-bounds read) by crafting a file that has fewer than 4 bytes.

CVE-2018-17292 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Fix out-of-bounds array access when passing a <4 byte input file to w… · WAVM/WAVM@2de6cf7	Patch Third Party Advisory github.com	MISC github.com/WAVM/WAVM/commit/2de6cf70c5ef31e22ed119a25ac2daeefd3d18a1

WAVM/WAVM@2de6cf7 · GitHub	text/html	
Mishandling input files with file length less than 4 bytes (crash) · Issue #109 · WAVM/WAVM · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/WAVM/WAVM/issues/109

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	Webassembly Virtual Machine Project	Webassembly Virtual Machine	All	All	All	All
Application	Webassembly Virtual Machine Project	Webassembly Virtual Machine	All	All	All	All

cpe:2.3:a:webassembly_virtual_machine_project:webassembly_virtual_machine:*:*:*:*:*:*:*:*:

cpe:2.3:a:webassembly_virtual_machine_project:webassembly_virtual_machine:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→