



CVE-2018-17293

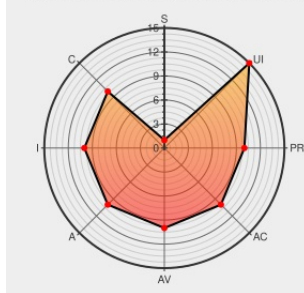
Published on: 09/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:20 PM UTC

CVE-2018-17293

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

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



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 run function in Programs/wavm/wavm.cpp does not check whether there is Emscripten memory to store the command-line arguments passed by the input WebAssembly file's main function, which allows attackers to cause a denial of service (application crash by NULL pointer dereference) or possibly have unspecified other impact by crafting certain WebAssembly files.

CVE-2018-17293 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Fix dereferencing null pointer when running wavm with	Patch Third Party Advisory	MISC github.com/WAVM/WAVM/commit/31d670b6489e6d708c3b04b911cdf14ac43d846d

WebAssembly mai... ·
WAVM/WAVM@31d670b ·
GitHub

github.com

text/html

Unhandled runtime exception:
wavm.reachedUnreachable
(sigabrt) · Issue #110 ·
WAVM/WAVM · GitHub

Exploit

Patch

Third Party Advisory

github.com

text/html

MISC [github.com/WAVM/WAVM/issues/110#issuecomment-421764693](#)

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 →