



CVE-2018-16767

Published on: 09/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

CVE-2018-16767

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

Certain versions of [Webassembly Virtual Machine](#) from [Webassembly Virtual Machine Project](#) contain the following vulnerability:

In WAVM through 2018-07-26, a crafted file sent to the WebAssembly Virtual Machine may cause a denial of service (application crash) or possibly have unspecified other impact because of an unspecified "heap-buffer-overflow" condition in `FunctionValidationContext::popAndValidateOperand`.

CVE-2018-16767 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
FunctionValidationContext::popAndValidateOperand(char const*, IR::ValueType) heap-buffer-overflow parsing running wasm file causing crash · Issue #97 · WAVM/WAVM · GitHub	Exploit Issue Tracking Patch Third Party Advisory	MISC github.com/AndrewScheidecker/WAVM/issues/97

Third Party Advisory
github.com
text/html

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →