



CVE-2018-20538

Published on: 12/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-20538

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

Certain versions of [Netwide Assembler](#) from [Nasm](#) contain the following vulnerability:

There is a use-after-free at `asm/preproc.c` (function `pp_getline`) in Netwide Assembler (NASM) 2.14rc16 that will cause a denial of service during certain finishes tests.

CVE-2018-20538 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
3392531 – There is a heap-use-after-free at <code>asm/preproc.c:5055</code> (function: <code>pp_getline</code>) in <code>nasm2.14rc16</code> that will cause dos attack.	Exploit Issue Tracking Third Party Advisory bugzilla.nasm.us text/html	MISC bugzilla.nasm.us/show_bug.cgi?id=3392531

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	Nasm	Netwide Assembler	2.14.0	rc16	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc16	All	All
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc16:*:*:*:*:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc16:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)