



CVE-2018-16517

Published on: 09/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16517

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

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

asm/labels.c in Netwide Assembler (NASM) is prone to NULL Pointer Dereference, which allows the attacker to cause a denial of service via a crafted file.

CVE-2018-16517 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
[security-announce] openSUSE-SU-2020:0954-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0954

[security-announce] openSUSE-SU-2020:0952-1:
moderate: Security update f

[Mailing List](#)
[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

 [SUSE openSUSE-SU-2020:0952](#)

Page not found · GitHub Pages

[Exploit](#)
[Third Party Advisory](#)
[fakhrizulkifli.github.io](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

 [MISC fakhrizulkifli.github.io/CVE-2018-16517.html](#)

Netwide Assembler (NASM) 2.14rc15 - NULL Pointer
Dereference (PoC) - Multiple dos Exploit

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

 [EXPLOIT-DB 46726](#)

3392513 – NULL Pointer Dereference in asm/labels.c

[Exploit](#)
[Issue Tracking](#)
[Third Party Advisory](#)
[bugzilla.nasm.us](#)
[text/html](#)

 [MISC bugzilla.nasm.us/show_bug.cgi?id=3392513](#)

Netwide Assembler (NASM) 2.14rc15 Null Pointer
Dereference ≈ Packet Storm

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
[packetstormsecurity.com](#)
[text/html](#)

 [MISC packetstormsecurity.com/files/152566/Netwide-Assembler-NASM-2.14rc15-Null-Pointer-Dereference.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	Nasm	Netwide Assembler	2.14	rc15	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc1	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc10	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc11	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc12	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc13	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc14	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc2	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc3	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc4	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc5	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc6	All	All

Application	Nasm	Netwide Assembler	2.14.0	rc7	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc8	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc9	All	All
Application	Nasm	Netwide Assembler	2.14	rc15	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc1	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc10	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc11	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc12	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc13	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc14	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc2	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc3	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc4	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc5	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc6	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc7	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc8	All	All
Application	Nasm	Netwide Assembler	2.14.0	rc9	All	All
Application	Nasm	Netwide Assembler	All	All	All	All
cpe:2.3:a:nasm:netwide_assembler:2.14:rc15:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc1:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc10:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc11:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc12:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc13:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc14:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc2:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc3:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc4:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc5:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc6:*****:						
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc7:*****:						

cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc8:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc9:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14:rc15:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc1:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc10:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc11:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc12:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc13:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc14:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc2:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc3:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc4:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc5:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc6:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc7:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc8:*****:
cpe:2.3:a:nasm:netwide_assembler:2.14.0:rc9:*****:
cpe:2.3:a:nasm:netwide_assembler:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)