



CVE-2017-17812

Published on: 12/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:26 PM UTC

CVE-2017-17812

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

In Netwide Assembler (NASM) 2.14rc0, there is a heap-based buffer over-read in the function `detoken()` in `asm/preproc.c` that will cause a remote denial of service attack.

CVE-2017-17812 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
USN-3694-1: NASM vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3694-1
Public Git Hosting - nasm.git/commit	Patch	MISC

Vendor Advisory

repo.or.cz

text/xml

repo.or.cz/nasm.git/commit/9b7ee09abfd426b99aa1ea81d19a3b2818eeabf9

3392424 – There is a heap based buffer overflow in function detoken() of nasm

Exploit

Issue Tracking

Vendor Advisory

bugzilla.nasm.us

text/html

 MISC bugzilla.nasm.us/show_bug.cgi?id=3392424

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
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Application	Nasm	Netwide Assembler	2.14	rc0	All	All
Application	Nasm	Netwide Assembler	2.14	rc0	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:its:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:its:*:*:

cpe:2.3:a:nasm:netwide_assembler:2.14:rc0:*:*:*:*:

cpe:2.3:a:nasm:netwide_assembler:2.14:rc0:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →