



CVE-2017-10686

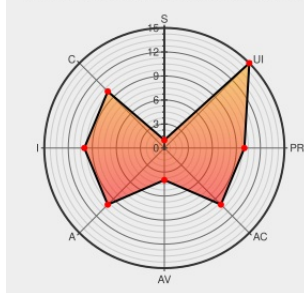
Published on: 06/29/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

CVE-2017-10686

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

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



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

In Netwide Assembler (NASM) 2.14rc0, there are multiple heap use after free vulnerabilities in the tool nasm. The related heap is allocated in the token() function and freed in the detoken() function (called by pp_getline()) - it is used again at multiple positions later that could cause multiple damages. For example, it causes a corrupted double-linked list in detoken(), a double free or corruption in delete_Token(), and an out-of-bounds write in detoken(). It has a high possibility to lead to a remote code execution attack.

CVE-2017-10686 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
NASM: Multiple vulnerabilities (CVE SA-201002-10)	Centos security	CentOS CVE SA-201002-10

NASM: Multiple vulnerabilities (GLSA 201903-19) — Gentoo security

security.gentoo.org
text/html

GENTOO GLSA-201903-19

USN-3694-1: NASM vulnerabilities | Ubuntu security notices

Third Party Advisory
usn.ubuntu.com
text/html

UBUNTU USN-3694-1

3392414 – Multiple use after free vulnerabilities in the Nasm tool with latest vesion

Exploit
Issue Tracking
Patch
Third Party Advisory
VDB Entry
bugzilla.nasm.us
text/html

MISC bugzilla.nasm.us/show_bug.cgi?id=3392414

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.

Related QID Numbers

710188 Gentoo Linux NASM Multiple vulnerabilities (GLSA 201903-19)

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

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report