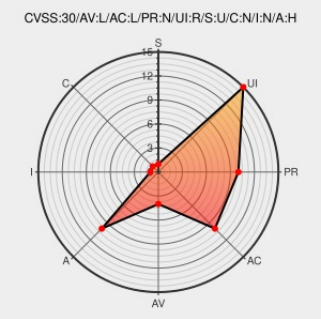
CVE-2017-17810

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

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

CVE-2017-17810

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 "SEGV on unknown address" that will cause a remote denial of service attack, because asm/preproc.c mishandles macro calls that have the wrong number of arguments.

CVE-2017-17810 has been assigned by 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
3392431 – There is a SEGV on unknown address 0x000000000018 in nasm.	Exploit, Issue Tracking, Vendor Advisory, bugzilla.nasm.us, text/html	MISC bugzilla.nasm.us/show_bug.cgi?id=3392431

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 Vendor Advisory repo.or.cz text/xml	MISC repo.or.cz/nasm.git/commit/59ce1c67b16967c652765e62aa130b7e43f21dd4

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:*:*:*:lts:*:*:*:

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

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→