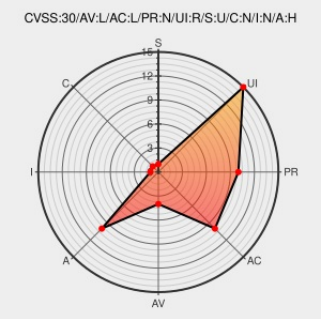
CVE-2018-19755

Published on: 11/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19755

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Netwide Assembler from Nasm contain the following vulnerability:

There is an illegal address access at asm/preproc.c (function: is_mmacro) in Netwide Assembler (NASM) 2.14rc16 that will cause a denial of service (out-of-bounds array access) because a certain conversion can result in a negative integer.

CVE-2018-19755 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
Public Git Hosting - nasm.git/commit	Exploit Third Party Advisory repo.or.cz text/xml	MISC repo.or.cz/nasm.git/commit/3079f7966dbed4497e36d5067cbfd896a90358cb

3392528 – There is an illegal address access at asm/preproc.c:4677(function:is_mmacro) in nasm2.14rc16 that will cause dos attack.	Exploit Issue Tracking Third Party Advisory bugzilla.nasm.us text/html	MISC bugzilla.nasm.us/show_bug.cgi?id=3392528

Related QID Numbers

670256 EulerOS Security Update for nasm (EulerOS-SA-2021-1820)

670915 EulerOS Security Update for nasm (EulerOS-SA-2020-2416)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nasm	Netwide Assembler	12.14	rc16	All	All
Application	Nasm	Netwide Assembler	12.14	rc16	All	All

cpe:2.3:a:nasm:netwide_assembler:12.14:rc16:*:*:*:*:*:*:

cpe:2.3:a:nasm:netwide_assembler:12.14:rc16:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→