



# NASM Netwide Assembler preproc.c parse\_\_smacro\_\_template null pointer dereference

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-8844                                                                                                                                                                                                                                                                                                                          |
| State           | PUBLISHED                                                                                                                                                                                                                                                                                                                              |
| Assigner        | VulDB                                                                                                                                                                                                                                                                                                                                  |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                           |
| Published       | 2025-08-11 12:15:26 UTC                                                                                                                                                                                                                                                                                                                |
| Updated         | 2026-04-29 01:00:01 UTC                                                                                                                                                                                                                                                                                                                |
| Description     | A vulnerability was determined in NASM Netwide Assembler 2.17rc0. This vulnerability affects the function parse__smacro__template in preproc.c. The vulnerability is a null pointer dereference that can be triggered by a specially crafted macro template. This can lead to a denial of service or potentially further exploitation. |

Risk And Classification

Primary CVSS: v4.0 1.9 LOW from cna@vulldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-404 | CWE-476 | CWE-476 NULL Pointer Dereference | CWE-404 Denial of Service

| Version | Source         | Type      | Score | Severity | Vector                                                                                                                                                                       |
|---------|----------------|-----------|-------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.0     | cna@vulldb.com | Secondary | 1.9   | LOW      | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0     | CNA            | DECLARED  | 4.8   | MEDIUM   | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 3.1     | nvd@nist.gov   | Primary   | 5.5   | MEDIUM   | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H                                                                                                                                 |
| 3.1     | cna@vulldb.com | Secondary | 3.3   | LOW      | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L                                                                                                                                 |
| 3.1     | CNA            | DECLARED  | 3.3   | LOW      | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R                                                                                                                   |
| 3.0     | CNA            | DECLARED  | 3.3   | LOW      | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R                                                                                                                   |
| 2.0     | cna@vulldb.com | Secondary | 1.7   |          | AV:L/AC:L/Au:S/C:N/I:N/A:P                                                                                                                                                   |
| 2.0     | CNA            | DECLARED  | 1.7   |          | AV:L/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:ND/RC:UR                                                                                                                                 |

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

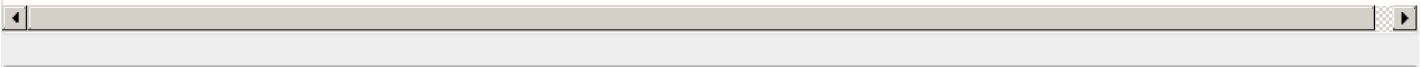
Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

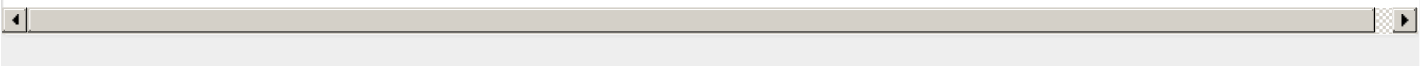
Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R



NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product           | Version | Update | Edition | Language |
|-------------|--------|-------------------|---------|--------|---------|----------|
| Application | Nasm   | Netwide Assembler | 2.17    | rc0    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product           | Version          | Platforms     |
|--------|--------|-------------------|------------------|---------------|
| CNA    | NASM   | Netwide Assembler | affected 2.17rc0 | Not specified |

References

| Reference                                                                      | Source                               | Link                             | Tags    |
|--------------------------------------------------------------------------------|--------------------------------------|----------------------------------|---------|
| vuldb.com                                                                      | cna@vuldb.com                        | <a href="#">vuldb.com</a>        | Exploit |
| vuldb.com                                                                      | cna@vuldb.com                        | <a href="#">vuldb.com</a>        | Permis  |
| vuldb.com                                                                      | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | <a href="#">vuldb.com</a>        | Exploit |
| vuldb.com                                                                      | cna@vuldb.com                        | <a href="#">vuldb.com</a>        | Exploit |
| <a href="#">drive.google.com/file/d/10TSdMErFTBtLFIwfh_fia635cmtmFuei/view</a> | cna@vuldb.com                        | <a href="#">drive.google.com</a> | Exploit |
| vuldb.com                                                                      | cna@vuldb.com                        | <a href="#">vuldb.com</a>        | Third F |
| <a href="#">bugzilla.nasm.us/show_bug.cgi</a>                                  | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | <a href="#">bugzilla.nasm.us</a> | Exploit |
| CVE Program record                                                             | CVE.ORG                              | <a href="#">www.cve.org</a>      | canoni  |
| NVD vulnerability detail                                                       | NVD                                  | <a href="#">nvd.nist.gov</a>     | canoni  |



Vendor Comments And Credit

**CNA:** xdcao (VulDB User) (en)

| Additional Advisory Data |                          |                         |
|--------------------------|--------------------------|-------------------------|
| Source                   | Time                     | Event                   |
| CNA                      | 2025-08-10T00:00:00.000Z | Advisory disclosed      |
| CNA                      | 2025-08-10T02:00:00.000Z | VulDB entry created     |
| CNA                      | 2025-08-10T18:02:10.000Z | VulDB entry last update |

There are currently no legacy QID mappings associated with this CVE.