Open5GS AMF Service nsmf-handler.c amf_nsmf_pdusession_handle_release_sm_context assertion

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-8698
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-07 21:15:29 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was found in Open5GS up to 2.7.5. It has been classified as problematic. Affected is the function amf_nsmf_

Risk And Classification

Primary CVSS: v4.0 1.9 LOW from cna@vuldb.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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-617 | CWE-617 Reachable Assertion

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.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/C...
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
3.1	cna@vuldb.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:O/RC:C
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:O/RC:C
2.0	cna@vuldb.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:OF/RC:C

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/MSC: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

Low

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

CVSS v3.0 Breakdown

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:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open5gs	Open5gs	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Open5GS	affected 2.7.0	Not specified
CNA	Na	Open5GS	affected 2.7.1	Not specified
CNA	Na	Open5GS	affected 2.7.2	Not specified
CNA	Na	Open5GS	affected 2.7.3	Not specified
CNA	Na	Open5GS	affected 2.7.4	Not specified
CNA	Na	Open5GS	affected 2.7.5	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Requ
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis
github.com/open5gs/open5gs/commit/66bc558e417e70ae216ec155e4e81c14ae0ecf30	cna@vuldb.com	github.com	Product
github.com/user-attachments/files/21356631/amf_nsmf_pdusession_handle_re...	cna@vuldb.com	github.com	Not Applicable
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis
github.com/open5gs/open5gs/issues/4012	cna@vuldb.com	github.com	Exploit, Issue Tra
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

CNA: SQ0409 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-08-07T00:00:00.000Z	Advisory disclosed
CNA	2025-08-07T02:00:00.000Z	VulDB entry created
CNA	2025-08-07T22:29:12.000Z	VulDB entry last update

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