Open5GS QER/FAR/URR/PDR context.c ogs_pfcp_qer_find_or_add assertion

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

Summary

CVE	CVE-2025-14954
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-19 16:15:55 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in Open5GS up to 2.7.6. Affected is the function ogs_pfcp_pdr_find_or_add/ogs_pfcp_far_fi

Risk And Classification

Primary CVSS: v4.0 2.9 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/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	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/C.
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	cna@vuldb.com	Secondary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.7	LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	2.6		AV:N/AC:H/Au:N/C:N/I:N/A:P
2.0	CNA	DECLARED	2.6		AV:N/AC:H/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/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

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:N/AC:H/PR:N/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
CNA	Na	Open5GS	affected 2.7.6	Not specified

References

Reference	Source	Link	Tags
github.com/open5gs/open5gs/issues/4181	cna@vuldb.com	github.com	Issue Tracking
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisc
github.com/open5gs/open5gs/issues/4181	cna@vuldb.com	github.com	Exploit, Issue Tra
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Requ
github.com/open5gs/open5gs/issues/4181	cna@vuldb.com	github.com	Exploit, Issue Tra
github.com/open5gs/open5gs/commit/442369dcd964f03d95429a6a01a57ed21f7779b7	cna@vuldb.com	github.com	Patch

github.com/open5gs/open5gs	cna@vuldb.com	github.com	
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

Vendor Comments And Credit

Discovery Credit

CNA: ZiyuLin (VulDB User) (en)

CNA: ZiyuLin (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-19T00:00:00.000Z	Advisory disclosed
CNA	2025-12-19T01:00:00.000Z	VulDB entry created
CNA	2025-12-28T18:41:55.000Z	VulDB entry last update

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