



Open5GS FAR-ID handler.c ogs_pfcpc_handle_create_pdr null pointer dereference

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-14953
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-19 16:15:54 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A flaw has been found in Open5GS up to 2.7.5. This impacts the function ogs_pfcpc_handle_create_pdr in the library lib/pfcpc

Risk And Classification

Primary CVSS: v4.0 1.3 LOW from cna@vulldb.com

CVSS:4.0/AV:N/AC:H/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	1.3	LOW	CVSS:4.0/AV:N/AC:H/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	2.3	LOW	CVSS:4.0/AV:N/AC:H/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	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	cna@vulldb.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.1	LOW	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
2.0	cna@vulldb.com	Secondary	2.1		AV:N/AC:H/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	2.1		AV:N/AC:H/Au:S/C:N/I:N/A:P/E:POC/RL:O/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

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:N/AC:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:N/AC:H/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
github.com/open5gs/open5gs/commit/93a9fd98a8baa94289be3b982028201de4534e32	cna@vuldb.com	github.com	Patch
github.com/open5gs/open5gs/issues/4179	cna@vuldb.com	github.com	Exploit, Issue Tracking
github.com/open5gs/open5gs/issues/4179	cna@vuldb.com	github.com	Issue Tracking
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory
github.com/open5gs/open5gs/issues/4179	cna@vuldb.com	github.com	Exploit, Issue Tracking

github.com/open5gs/open5gs/issues/7170	cna@vuldb.com	github.com	Exploit, issue title
github.com/open5gs/open5gs	cna@vuldb.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit
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	2025-12-25T02:21:53.000Z	VulDB entry last update

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