



Open5GS GTPv2-C F-TEID s11-handler.c sgwc_s11_handle_create_session_request denial of service

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-15417
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-01 23:15:56 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was identified in Open5GS up to 2.7.6. Affected is the function sgwc_s11_handle_create_session_request o

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-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/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	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: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@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: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/MSX/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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

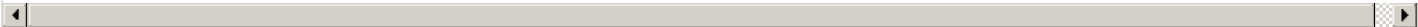
Integrity

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
CNA	Na	Open5GS	affected 2.7.6	Not specified

References

Reference	Source	Link
vuldb.com	cna@vuldb.com	vuldb.com
github.com/open5gs/open5gs/issues/4203	cna@vuldb.com	github.com
github.com/open5gs/open5gs/commit/465273d13ba5d47b274c38c9d1b07f04859178a1	cna@vuldb.com	github.com
github.com/open5gs/open5gs/issues/4203	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/open5gs/open5gs/issues/4203	cna@vuldb.com	github.com

vuldb.com	cna@vuldb.com	vuldb.c
vuldb.com	cna@vuldb.com	vuldb.c
github.com/open5gs/open5gs	cna@vuldb.com	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

--	--	--

Vendor Comments And Credit

Discovery Credit
CNA: ZiyuLin (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-01T00:00:00.000Z	Advisory disclosed
CNA	2026-01-01T01:00:00.000Z	VulDB entry created
CNA	2026-01-06T17:41:47.000Z	VulDB entry last update

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