Open5GS NSSF conv.c ogs_sbi_parse_plmn_list denial of service

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

Summary

CVE	CVE-2026-8121
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 01:16:09 UTC
Updated	2026-05-11 14:26:39 UTC
Description	A vulnerability has been found in Open5GS up to 2.7.7. The impacted element is the function ogs_sbi_parse_plmn_list in th

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@vuldb.com

CVSS:4.0/AV:N/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

EPSS: 0.000490000 probability, percentile 0.153670000 (date 2026-05-12)

Problem Types: CWE-404 | CWE-404 Denial of Service

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/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	5.3	MEDIUM	CVSS:4.0/AV:N/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	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	cna@vuldb.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	4.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	4		AV:N/AC:L/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	4		AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

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:N/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

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:N/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	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
CNA	Na	Open5GS	affected 2.7.7	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/361908/cti	cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry
vuldb.com/vuln/361908	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
vuldb.com/submit/808422	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry, Exploit
vuldb.com/submit/808424	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry

github.com/open5gs/open5gs/issues/4433	cna@vuldb.com	github.com	Exploit, Issue Tracking
github.com/open5gs/open5gs	cna@vuldb.com	github.com	Product
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: FrankyLin (VulDB User) (en)

CNA: VulDB CNA Team (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-07T00:00:00.000Z	Advisory disclosed
CNA	2026-05-07T02:00:00.000Z	VulDB entry created
CNA	2026-05-07T19:02:02.000Z	VulDB entry last update

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