VDB-343795 · CVE-2025-15555 · ISSUE 4177

OPEN5GS UP TO 2.7.6 VOLTE CX-TEST SRC/HSS/HSS-CX-PATH.C HSS_OGS_DIAM_CX_MAR_CB OGS_KEY_LEN STACK-BASED OVERFLOW

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

7.5 | $0-$5k | 0.33

Summary

A vulnerability marked as critical has been reported in Open5GS up to 2.7.6. Affected by this issue is the function `hss_ogs_diam_cx_mar_cb` of the file *src/hss/hss-cx-path.c* of the component *VoLTE Cx-Test*. This manipulation of the argument *OGS_KEY_LEN* causes stack-based overflow. This vulnerability is registered as CVE-2025-15555. Remote exploitation of the attack is possible. No exploit is available. To fix this issue, it is recommended to deploy a patch.

Details

A vulnerability has been found in Open5GS up to 2.7.6 and classified as critical. Affected by this vulnerability is the function `hss_ogs_diam_cx_mar_cb` of the file *src/hss/hss-cx-path.c* of the component *VoLTE Cx-Test*. The manipulation of the argument `OGS_KEY_LEN` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is CWE-121. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was published by Luca Jungnickel with Fraunhofer FOKUS as *4177*. It is possible to read the advisory at github.com. This vulnerability is known as CVE-2025-15555. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details of the vulnerability are known, but there is no available exploit.

Applying the patch 54dda041211098730221d0ae20a2f9f9173e7a21 is able to eliminate this problem. The bugfix is ready for download at github.com.

Similar entry is available at VDB-287066.

Product

Name

- Open5GS

Version

- 2.7.0
- 2.7.1
- 2.7.2
- 2.7.3
- 2.7.4
- 2.7.5
- 2.7.6

License

- open-source

Website

- Product: https://github.com/open5gs/open5gs/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 7.6
VulDB Meta Temp Score: 7.5

VulDB Base Score: 7.3
VulDB Temp Score: 7.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

NVD Base Score: 8.2
NVD Vector: 🔒

CNA Base Score: 7.3
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Stack-based overflow
CWE: CWE-121 / CWE-119
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Status: Not defined

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Patch
Status: 🔍

0-Day Time: 🔒

Patch: 54dda041211098730221d0ae20a2f9f9173e7a21

Timeline

02/02/2026		Advisory disclosed
02/02/2026	+0 days	VulDB entry created
04/07/2026	+64 days	VulDB entry last update

Sources

Product: github.com

Advisory: 4177
Researcher: Luca Jungnickel
Organization: Fraunhofer FOKUS
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2025-15555 (🔒)
GCVE (CVE): GCVE-0-2025-15555

GCVE (VulDB): GCVE-100-343795
See also: 🔒

Entry

Created: 02/02/2026 08:07 PM
Updated: 04/07/2026 05:49 PM
Changes: 02/02/2026 08:07 PM (58), 02/05/2026 01:48 PM (30), 02/12/2026 08:06 AM (11), 04/07/2026 05:49 PM (3)
Complete: 🔍
Submitter: jungnickel
Committer: jungnickel
Cache ID: 40:C52:179

Submit

Accepted

- Submit #741901: Open5GS v2.7.6 Buffer Over-read (by jungnickel)

Discussion

No comments yet. Languages: en.

Please log in to comment.