



Home > Submit > 741901

Submit #741901: Open5GS v2.7.6 Buffer Over-read

Title Open5GS v2.7.6 Buffer Over-read

Description Open5GS version 2.7.6 suffers from a buffer overread, which has been disclosed and acknowledged by the developers and fixed.

For reproduction, this can be triggered by executing the VoLTE CX Test, like described in the Github Issue (<https://github.com/open5gs/open5gs/issues/4177>).

The stack buffer ak is logged using OGS_KEY_LEN, but it is allocated with the shorter OGS_AK_LEN. This leads to a stack buffer overread, which is being logged. This mismatch causes a stack buffer over-read during logging, potentially leading to instability or information leakage. This is potentially remotely triggerable.

Source <https://github.com/open5gs/open5gs/issues/4177>

User jungnickel (UID 94661)

Submission 01/19/2026 10:29 AM (3 months ago)

Moderation 02/02/2026 08:02 PM (14 days later)

Status Accepted

VulDB entry 343796 [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]

Points 20

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)