



ESPILON
SECURITY RESEARCH

SECURITY ADVISORY

Out-of-bounds read in the Open5GS SUCI de-concealment parser

CVE-2026-116544

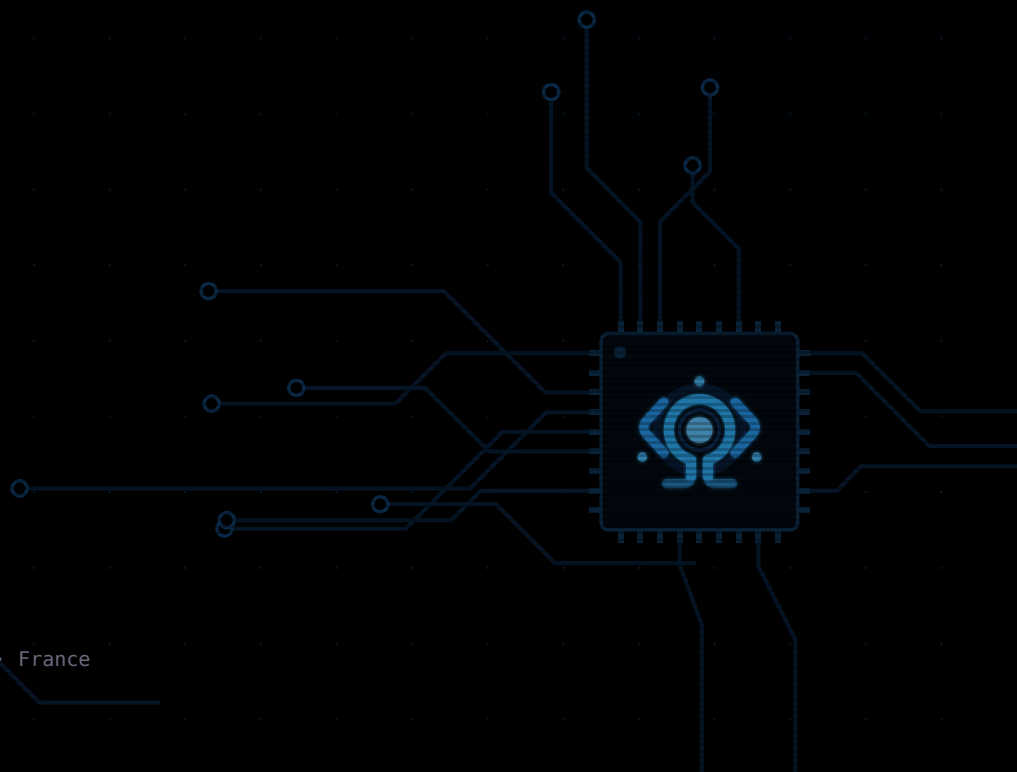
CVSS 6.3 • MEDIUM

Open5GS • UDM

CVE PUBLISHED 26 Oct 2026

Marouane El Moufid (Eun0us)

espilon.net • Association loi 1901 • France



01 Vulnerability

6.3

MEDIUM

CVSS 4.0 BASE SCORE · VULNCHECK (CNA)

AV:N / AC:H / AT:P / PR:N / UI:N / VC:L / VI:N / VA:N / SC:N / SI:N / SA:N
CVSS 3.1: 3.7 (Low) · AV:N / AC:H / PR:N / UI:N / S:U / C:L / I:N / A:N

CVE	CVE-2026-116544
Component	Open5GS, SUCI de-concealment (parse_scheme_output, lib/sbi/conv.c)
Affected	Open5GS 2.6.1 through 2.8.0
Fixed	Commit fdddc5e (Fix SUCI scheme-output length validation); no tagged release yet
Type	Heap out-of-bounds read (CWE-125)
Advisory	GHSA-vp5f-rg8g-8p7j
Credit	Epsilon · Marouane El Moufid (Eun0us)

Issue

When a handset first contacts a 5G network it does not send its permanent identifier (the SUPI, the 5G equivalent of the IMSI) in the clear. It sends a SUCI, the Subscription Concealed Identifier, an encrypted form that only the home network can open. On the network side the UDM, through its SIDF function, de-conceals the SUCI using the home network's private key. Open5GS parses the SUCI's scheme output (the attacker-supplied ephemeral public key, ciphertext and MAC) during that step. The minimum-length check on the scheme output omits the 5-byte ciphertext, so a 42-byte scheme output is accepted and the parser reads the MAC tag 3 to 4 bytes past the end of its heap copy.

Timeline

DATE	EVENT
2026-09-25	Fix committed (fdddc5e); GHSA-vp5f-rg8g-8p7j published
2026-10-26	CVE-2026-116544 published by VulnCheck (CNA)

Mitigation

No tagged release contains the fix yet (latest: v2.8.0). Build from main at or after commit fdddc5e, which requires the full key, ciphertext and MAC length before the de-concealment parse. The exposure exists only on deployments where the UDM is provisioned with home-network private keys, i.e. where SUCI de-concealment is actually performed.

02 Technical analysis

Root cause

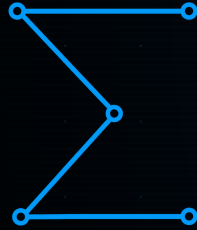
`parse_scheme_output()` in `lib/sbi/conv.c` sizes the scheme output from the hex string it receives (`strlen/2`) and rejects it only if it is at most $(\text{OGS_ECCKEY_LEN}+1) + \text{OGS_MACTAG_LEN} = 41$ bytes. The guard omits the 5-byte ciphertext (`OGS\_MSIN\_LEN`). A 42-byte scheme output passes and is copied into a 42-byte heap buffer. The parser then takes the ECC key (32 or 33 bytes), the 5-byte ciphertext and the 8-byte MAC tag, and the final `memcpy` of the MAC tag reads 3 bytes (profile A) or 4 bytes (profile B) past the allocation. Commit fdddc5e moves the check after the profile is known, requires `ecckey->size + OGS\_MSIN\_LEN + OGS\_MACTAG\_LEN` bytes, and widens `scheme_output_size` from `uint8_t` to `size_t`.

Reachability

The SUCI is carried in the initial registration request a handset sends when it attaches to the network, before authentication, since de-concealing it is how the network first learns which subscriber is attaching. A rogue or modified handset within radio range can therefore place a crafted SUCI on the air and reach the parser pre-authentication. The path is configuration-gated: the de-concealment routine runs only when the UDM holds the home-network private keys. Where those keys are provisioned, the read is reachable; where they are not, the path is not exercised, which is why this is scored below the SBI write.

Impact

A read of 3 or 4 bytes past a 42-byte heap allocation. The bytes go into the MAC tag buffer and are not returned on the wire; no crash was demonstrated. The CNA scores a low confidentiality impact only.



ESPILON

SECURITY RESEARCH

Embedded, IoT and OT security research

espilon.net

eun0us@espilon.net

Association loi 1901 • France