



ESPILON
SECURITY RESEARCH

SECURITY ADVISORY

Pre-auth heap out-of-bounds write in the Open5GS SBI multipart parser

CVE-2026-116543

CVSS 8.7 · HIGH

Open5GS · SBI

CVE PUBLISHED 26 Oct 2026

Marouane El Moufid (Eun0us)

espilon.net · Association loi 1901 · France



01 Vulnerability

8.7

HIGH

CVSS 4.0 BASE SCORE · VULNCHECK (CNA)

AV:N / AC:L / AT:N / PR:N / UI:N / VC:N / VI:N / VA:H / SC:N / SI:N / SA:N

CVSS 3.1: 7.5 (High) · AV:N / AC:L / PR:N / UI:N / S:U / C:N / I:N / A:H

CVE	CVE-2026-116543
Component	Open5GS, SBI HTTP multipart parser (lib/sbi/contrib/multipart_parser.c, parse_multipart in lib/sbi/message.c)
Affected	Open5GS 1.3.0 through 2.8.0
Fixed	Commit 6820c274 (Reject empty multipart boundaries); no tagged release yet
Type	Heap out-of-bounds write (CWE-787) via an empty multipart boundary
Advisory	GHSA-25v2-v588-jq8g
Credit	Epsilon · Marouane El Moufid (Eun0us)

Issue

Open5GS is an open-source implementation of the 5G core (and 4G EPC). Its network functions talk to each other over the SBI (Service Based Interface), the HTTP/2 control plane that carries the signalling of the core. Some SBI messages use HTTP multipart bodies to carry binary artifacts alongside their JSON. The multipart parser that splits those bodies mishandles a request whose declared boundary delimiter is empty: the boundary match never completes, its index keeps growing, and the parser writes past the end of its heap allocation. A single crafted HTTP request, with no authentication, corrupts the heap of the receiving network function and crashes it.

Timeline

DATE	EVENT
2026-09-25	Fix committed (6820c274); GHSA-25v2-v588-jq8g published
2026-10-26	CVE-2026-116543 published by VulnCheck (CNA)

Mitigation

No tagged release contains the fix yet (latest: v2.8.0). Build from main at or after commit 6820c274, which rejects an empty boundary before the parser is initialised. Keep the SBI off untrusted networks and require mutual TLS; OAuth2 access tokens do not mitigate this, as the request is parsed before the token is checked.

02 Technical analysis

Root cause

The multipart parser (lib/sbi/contrib/multipart_parser.c) is a byte-at-a-time state machine. multipart_parser_init() allocates the parser and its lookbehind buffer in one heap block sized from strlen(boundary), and sets boundary_length = strlen(boundary). In state s_part_data_boundary each byte is stored with p->lookbehind[2 + p->index] = c, and the state ends when ++p->index == p->boundary_length. parse_multipart() in lib/sbi/message.c extracts the boundary with ogs_strndup() and never checks its length. A body of the form CRLF CRLF yields an empty boundary, so boundary_length is 0 and the equality is never reached:

p->index grows without bound and the store runs linearly past the end of the heap block (multipart_parser.c:260 in v2.8.0).

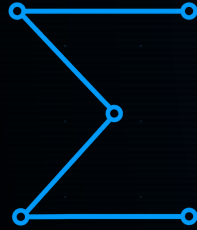
The fix is to reject an empty boundary up front, before the parser is initialised, which is exactly what commit 6820c274 ("Reject empty multipart boundaries") does.

Reachability

The SBI is the inter-NF control plane of the 5G core. The multipart parser runs when a network function receives an SBI request with a multipart body, and the empty-boundary path is taken before any application-level authentication of the message contents. In a deployment where an attacker can reach a core NF's SBI endpoint, directly, through a misconfigured gateway, or from a compromised neighbouring function, the request needs no credentials and no prior state. This is the pre-authentication position on the SBI network that the AV:N / PR:N vector reflects.

Impact

The out-of-bounds store writes a fixed, periodic byte pattern, not attacker-chosen data. The demonstrated and reliable outcome is a crash of that function, a denial of service of a component of the 5G core control plane. Heap corruption of this shape is not, on its own, a proof of code execution, and none is claimed here; the scored and demonstrated impact is availability.



ESPILON

SECURITY RESEARCH

Embedded, IoT and OT security research

espilon.net

eun0us@espilon.net

Association loi 1901 • France