



ESPILON
SECURITY RESEARCH

SECURITY ADVISORY

Out-of-bounds read in the LibOSDP file-transfer decoder

CVE-2026-77275

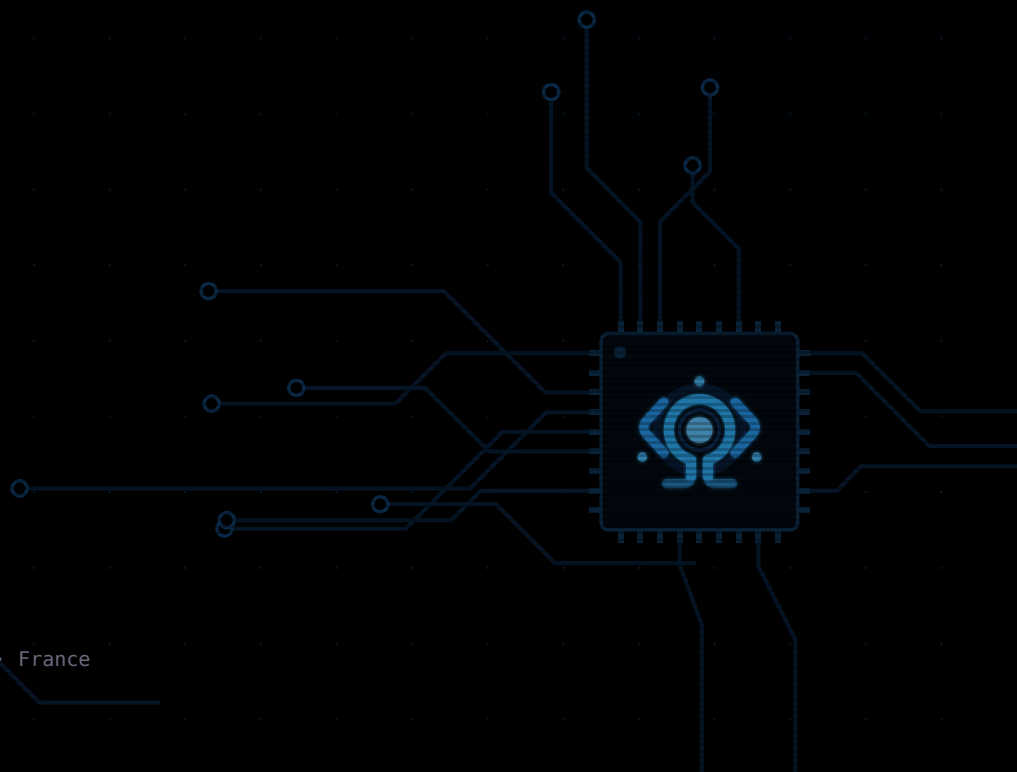
CVSS 6.5 • MEDIUM

LibOSDP • libosdp

ADVISORY PUBLISHED 30 Aug 2026

Marouane El Moufid (Eun0us)

espilon.net • Association loi 1901 • France



01 Vulnerability

6.5

CVSS 3.1 BASE SCORE

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

MEDIUM

CVE	CVE-2026-77275
Component	LibOSDP, file-transfer command decoder <code>osdp_file_cmd_tx_decode</code>
Affected	LibOSDP >= 2.0.0
Fixed	LibOSDP 3.2.4
Type	Out-of-bounds read (CWE-125)
Advisory	GHSA-23h3-j4q9-8hf6
Credit	Epsilon · Marouane El Moufid (Eun0us)

Issue

LibOSDP is an open-source implementation of OSDP, the protocol an access-control control panel uses to talk to its card readers over an RS-485 bus. Its file-transfer decoder, `osdp_file_cmd_tx_decode()`, reads a 16-bit payload length verbatim from an incoming `CMD_FILETRANSFER` command and hands it to the write handler without checking it against the number of bytes actually received. A frame that advertises a large length but carries few data bytes makes the handler read far past the end of the receive buffer, a reliable denial of service of the reader (PD).

Timeline

DATE	EVENT
2026-07-10	LibOSDP v3.2.4 released with the fix
2026-08-30	Advisory GHSA-23h3-j4q9-8hf6 published

Mitigation

Update to LibOSDP 3.2.4, which validates the advertised file-transfer length against the bytes actually received before dispatching. Enforce Secure Channel (`OSDP_FLAG_ENFORCE_SECURE`) to remove the pre-authentication reachability on the bus.

02 Technical analysis

`osdp_file_cmd_tx_decode()` parses an incoming `CMD_FILETRANSFER` command, reads a 16-bit payload length straight from the wire, and passes that length to the registered write handler without checking it against the number of bytes the frame actually carried. The only consistency check present is an `assert()`, which is compiled out under `NDEBUG`, the normal release build.

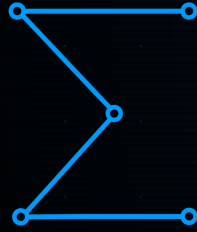
A frame advertising a large length but carrying few data bytes makes the write handler read far past the end of the PD receive buffer, up to roughly 64 KiB, faulting once it crosses an unmapped page. This is a reliable reader denial of service.

Confidentiality

The over-read bytes are handed to the integrator's local write handler and consumed internally, typically persisted to the received file. They are not reflected back onto the OSDP wire, so there is no remote read-back channel. It is a crash, not an information leak, which is why confidentiality is scored none.

Reachability

The PD command dispatcher routes a plaintext `CMD_FILETRANSFER` into the decoder when Secure Channel is not enforced (`OSDP_FLAG_ENFORCE_SECURE` unset, the default). The attacker is on the RS-485 bus and speaks as the control panel: a rogue CP, a tapped bus, or an in-line serial-to-IP bridge injecting CRC-valid commands. A transfer must be in progress, which the attacker opens itself (two back-to-back frames). No pairing, key or prior handshake is needed.



ESPILON

SECURITY RESEARCH

Embedded, IoT and OT security research

espilon.net

eun0us@espilon.net

Association loi 1901 • France