OOB read in ptp_unpack_OI() in ptp-pack.c via malicious PTP ObjectInfo response

Moderate **msmeissn** published **GHSA-xfw3-xvjp-5wcv** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

An out-of-bounds read vulnerability exists in ptp_unpack_OI() in camlibs/ptp2/ptp-pack.c (lines 530–563). The function validates `len < PTP_oi_SequenceNumber` (i.e., len < 48) but subsequently accesses offsets 48–56, up to 9 bytes beyond the validated boundary, via the Samsung Galaxy 64-bit objectsize detection heuristic.

Tested against commit `dc49f1b`.

Attack Scenario

A malicious USB device or rogue PTP/IP network endpoint sends a crafted PTP ObjectInfo response with len < 57. On Linux with GNOME, gvfs auto-mounts PTP devices via libgphoto2 without user interaction (zero-click on default Ubuntu/Fedora desktop).

ptp_unpack_OI() is called for every file listing operation on any PTP device, making this the most directly exploitable finding in the codebase.

Technical Details

File: camlibs/ptp2/ptp-pack.c, lines 530–563

The function validates:
if (!data || len < PTP_oi_SequenceNumber) // PTP_oi_SequenceNumber = 48

But then accesses:

- Offsets 48–51: dtoh32a(data + PTP_oi_SequenceNumber): 4 bytes OOB
- Offset 52: data[PTP_oi_filenamelen] : 5 bytes OOB
- Offset 56: data[PTP_oi_filenamelen + 4] : 9 bytes OOB

These reads can expose adjacent heap memory contents from PTP response buffers allocated by untrusted device data.

Suggested Fix

- if (!data || len < PTP_oi_SequenceNumber)
- if (!data || len < PTP_oi_filenamelen + 5)

Impact

Heap memory disclosure via adjacent buffer contents. CWE-125.
The project's SECURITY.md explicitly states USB/PTP-IP device data is untrusted and memory corruption is in scope.

Severity

Moderate 6.1 / 10

CVSS v3 base metrics

Attack vector	Physical
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE ID

CVE-2026-40340

Weaknesses

▶ CWE-125

Credits

 **Sebasteuo** Reporter