OOB read in ptp_unpack_Sony_DPD() enumeration count parsing in ptp-pack.c

Moderate **msmeissn** published **GHSA-2hwp-w84q-27hf** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

An out-of-bounds read exists in the PTP_DPFF_Enumeration case of ptp_unpack_Sony_DPD() in camlibs/ptp2/ptp-pack.c (line 856). The function reads a 2-byte enumeration count N via dtoh16o(data, *poffset) without verifying that 2 bytes remain in the buffer.

The standard ptp_unpack_DPD() at line 704 has this exact check, confirming the Sony variant omitted it by oversight.

Tested against commit `dc49f1b`.

Attack Scenario

A rogue PTP/IP server or malicious USB device sends a crafted Sony Device Property Descriptor with FormFlag = PTP_DPFF_Enumeration and a truncated buffer. The host reads 2 bytes beyond the buffer boundary when parsing the enumeration count, exposing adjacent heap memory.

Technical Details

File: camlibs/ptp2/ptp-pack.c, line 856

Standard DPD parser (CORRECT):
if (*offset + sizeof(uint16_t) > dpdlen) goto outofmemory;
N = dtoh16o(data, *offset);

Sony DPD parser (VULNERABLE):
// No bounds check before this read:
N = dtoh16o(data, *poffset);

This is a distinct vulnerability from the FormFlag OOB read (line 842) — it occurs in a different code path (PTP_DPFF_Enumeration case), reads 2 bytes instead of 1, and requires a different fix.

Suggested Fix

case PTP_DPFF_Enumeration: {

- if (*poffset + sizeof(uint16_t) > dpdlen) goto outofmemory;
  N = dtoh16o(data, *poffset);

Impact

Two bytes of adjacent heap memory disclosure during property enumeration on Sony devices. CWE-125. Independently fixable from all other findings in this codebase.

Severity

Moderate 5.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-40338

Weaknesses

▶ CWE-125

Credits

 **Sebasteuo** Reporter