# OOB read in ptp_unpack_Sony_DPD() FormFlag parsing in ptp-pack.c

Moderate **msmeissn** published **GHSA-42cm-m9hc-r7q8** 3 days ago

**Package**

**libgphoto2**

**Affected versions**

<= 2.5.33

**Patched versions**

None

**Description**

## Summary

An out-of-bounds read exists in ptp_unpack_Sony_DPD() in camlibs/ptp2/ptp-pack.c (line 842). The function reads the FormFlag byte via dtoh8o(data, *poffset) without a prior bounds check.

The standard ptp_unpack_DPD() at lines 686–687 correctly validates *offset + sizeof(uint8_t) > dpdlen before this same read, but the Sony variant omits this check entirely.

Tested against commit `dc49f1b`.

## Attack Scenario

A rogue PTP/IP server or malicious USB device sends a crafted Sony Device Property Descriptor with a truncated buffer. When the host enumerates device properties, ptp_unpack_Sony_DPD() reads one byte beyond the buffer boundary, exposing adjacent heap memory.

## Technical Details

File: camlibs/ptp2/ptp-pack.c, line 842

Standard DPD parser (CORRECT):
if (*offset + sizeof(uint8_t) > dpdlen)
return 1;
dpd->FormFlag = dtoh8o(data, *offset);

Sony DPD parser (VULNERABLE):
// No bounds check before this read:
dpd->FormFlag = dtoh8o(data, *poffset);

The inconsistency confirms this was an oversight — the correct pattern was already established in the same file.

## Suggested Fix

if (*poffset == PTP_dpd_Sony_DefaultValue)
return 1;

- if (*poffset + sizeof(uint8_t) > dpdlen)
- ```
  return 1;
  ```

  dpd->FormFlag = dtoh8o(data, *poffset);

## Impact

One byte of adjacent heap memory disclosure per property enumeration.
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-2026-40339

### Weaknesses

▶ CWE-125

### Credits

**Sebasteuo** Reporter