Memory leak in ptp_unpack_Sony_DPD() secondary enumeration list in ptp-pack.c

Low **msmeissn** published **GHSA-g8xw-p5wj-mrxv** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

A memory leak exists in ptp_unpack_Sony_DPD() in camlibs/ptp2/ptp-pack.c (lines 884–885). When processing a secondary enumeration list (introduced in 2024+ Sony cameras), the function overwrites dpd->FORM.Enum.SupportedValue with a new calloc() without freeing the previous allocation from line 857. The original array and any string values it contains are leaked on every property descriptor parse.

Tested against commit `dc49f1b`.

Technical Details

File: camlibs/ptp2/ptp-pack.c, lines 884–885

First allocation (line 857) never freed:
dpd->FORM.Enum.SupportedValue = calloc(N,
sizeof(dpd->FORM.Enum.SupportedValue[0]));

Overwrite without free (lines 884–885):
N = dtoh16o(data, *poffset);
dpd->FORM.Enum.SupportedValue = calloc(N,
sizeof(dpd->FORM.Enum.SupportedValue[0]));

A malicious device can trigger repeated property descriptor responses, causing unbounded heap growth and eventual memory exhaustion in the host process.

Suggested Fix

N = dtoh16o(data, *poffset);

- free(dpd->FORM.Enum.SupportedValue);
- dpd->FORM.Enum.SupportedValue = NULL;
  dpd->FORM.Enum.SupportedValue = calloc(N,
  sizeof(dpd->FORM.Enum.SupportedValue[0]));

Impact

Heap memory exhaustion via repeated crafted Sony property descriptor responses. A malicious device can cause the libgphoto2 host process to consume unbounded memory. CWE-401. Independently fixable from all other findings.

Severity

Low 2.4 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-40336

Weaknesses

▶ CWE-401

Credits

Sebasteuo Reporter