OOB read in ptp_unpack_EOS_ImageFormat() and ptp_unpack_EOS_CustomFuncEx() due to missing length parameter in ptp-pack.c

Moderate **msmeissn** published **GHSA-hq94-cp6h-3gjp** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

Two functions in camlibs/ptp2/ptp-pack.c accept a data pointer
but no length parameter, performing unbounded reads:

- ptp_unpack_EOS_ImageFormat() at line 1457: up to 36 bytes
- ptp_unpack_EOS_CustomFuncEx() at line 1677: up to 1024 bytes

Their callers in ptp_unpack_EOS_events() have xsize available
but never pass it, leaving both functions unable to validate
reads against the actual buffer boundary.

Tested against commit `dc49f1b`.

Attack Scenario

A malicious USB device or rogue PTP/IP server sends a crafted EOS event response with a truncated buffer. Either function will read beyond the buffer boundary — up to 1024 bytes in the CustomFuncEx case — exposing adjacent heap memory.

Technical Details

File: camlibs/ptp2/ptp-pack.c

ptp_unpack_EOS_ImageFormat() line 1457:
static int ptp_unpack_EOS_ImageFormat(
PTPParams *params,*
*const unsigned char** data)
// No length parameter — performs up to 36 bytes
// of dtoh32o reads without bounds validation

ptp_unpack_EOS_CustomFuncEx() line 1677:
static int ptp_unpack_EOS_CustomFuncEx(
PTPParams *params,*
*const unsigned char** data)
// No length parameter — performs up to 1024 bytes
// of reads without bounds validation

Callers in ptp_unpack_EOS_events() have xsize available but pass only the data pointer.

Suggested Fix

Add a datasize parameter to both functions and validate all internal reads against it:

```
static int ptp_unpack_EOS_ImageFormat(
    PTPParams *params,
    const unsigned char** data,
    uint32_t datasize)

static int ptp_unpack_EOS_CustomFuncEx(
    PTPParams *params,
    const unsigned char** data,
    uint32_t datasize)
```

Update all callers to pass xsize accordingly.

Impact

Up to 1024 bytes of adjacent heap memory disclosure via crafted EOS event responses. The CustomFuncEx variant is the most severe due to the large potential read range.
CWE-125. Independently fixable from all other findings.

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-2026-40333

Weaknesses

▶ CWE-125

Credits

 **Sebasteuo** Reporter