OOB read in ptp_unpack_DPV() UINT128/INT128 handling in ptp-pack.c

Moderate **msmeissn** published **GHSA-g4g5-c2x9-cqfj** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

An out-of-bounds read exists in ptp_unpack_DPV() in camlibs/ptp2/ptp-pack.c (lines 622–629). The UINT128 and INT128 cases advance *offset += 16 without verifying that 16 bytes remain in the buffer. The entry check at line 609 only guarantees *offset < total (at least 1 byte available), leaving up to 15 bytes unvalidated.

Tested against commit `dc49f1b`.

Attack Scenario

A rogue PTP/IP server or malicious USB device sends a crafted Device Property Value with datatype PTP_DTC_UINT128 or PTP_DTC_INT128 and a buffer smaller than 16 bytes. The offset advances beyond the buffer boundary. The subsequent CTVAL macro bounds check (total - *offset < sizeof(target)) wraps due to unsigned arithmetic, bypassing the intended protection.

Technical Details

File: camlibs/ptp2/ptp-pack.c, lines 622–629

Entry check (line 609) insufficient:
if (*offset >= total) return 0; // only guarantees 1 byte

Vulnerable cases:
case PTP_DTC_UINT128:
*offset += 16; // no check that 16 bytes remain
break;
case PTP_DTC_INT128:
*offset += 16; // no check that 16 bytes remain
break;

After the unchecked advance, *offset > total causes unsigned wraparound in subsequent CTVAL bounds checks, defeating them.

Suggested Fix

Add a bounds check before each 16-byte offset advance:

```
case PTP_DTC_UINT128:
    if (total - *offset < 16)
        return 0;
    *offset += 16;
    break;
case PTP_DTC_INT128:
    if (total - *offset < 16)
        return 0;
    *offset += 16;
    break;
```

Impact

Up to 16 bytes of adjacent heap memory disclosure per crafted property value response. The unsigned wraparound additionally defeats downstream bounds checks. 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-2026-40335

Weaknesses

▶ CWE-125

Credits

Sebasteuo Reporter