gphoto / **libgphoto2** Public

Code Issues 441 Pull requests 16 Actions Projects Wiki Sec

Commit 433bde9

msmeissn committed 3 days ago · ✓ 4 / 4

```
Fixed UINT128/INT128 Unchecked Offset Advance (CWE-125) — MEDIUM

Finding 5: UINT128/INT128 Unchecked Offset Advance (CWE-125) — MEDIUM

In ptp_unpack_DPV(), the PTP_DTC_UINT128 and PTP_DTC_INT128 cases advance *offset += 16
without verifying 16 bytes remain. The entry check at line 609 only guarantees *offset < total
(at least 1 byte available). After the unchecked advance, *offset can exceed total, and the
CTVAL macro's bounds check (total - *offset < sizeof(target)) wraps due to unsigned
arithmetic.

CVE-2026-40335

Reported-By: Sebastián Alba <sebasjosue84@gmail.com>
```

master

1 parent 259fc7d commit 433bde9

1 file changed +4 -0 lines changed

Top

Filter files…

camlibs/ptp2

ptp-pack.c

1 file changed +4 -0 lines changed

Search within code

camlibs/ptp2/ptp-pack.c

```
@@ -620,10 +620,14 @@ ptp_unpack_DPV (
620  620        case PTP_DTC_UINT64: CTVAL(value->u64,dtoh64a); break;
621  621
622  622        case PTP_DTC_UINT128:
     623  +         if (total - *offset < 16)
```

```
                624 +               return 0;
623             625                 *offset += 16;
624             626                 /*fprintf(stderr,"unhandled unpack of uint128n");*/
625             627                 break;
626             628             case PTP_DTC_INT128:
                629 +               if (total - *offset < 16)
                630 +                   return 0;
627             631                 *offset += 16;
628             632                 /*fprintf(stderr,"unhandled unpack of int128n");*/
629             633                 break;
```

Comments 0

Please sign in to comment.