gphoto / **libgphoto2** Public

Code Issues 441 Pull requests 16 Actions Projects Wiki Sec

Commit `404ff02`

msmeissn committed 3 days ago · ✓ 4 / 4

```
Fixed Sony DPD Secondary Enum List Memory Leak

Finding 4: Sony DPD Secondary Enum List Memory Leak (CWE-401) — LOW

File: ptp-pack.c:884-885

When processing a secondary enumeration list (2024+ Sony cameras), line
884–885 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.

CVE-2026-40336

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

master

1 parent 50a2da6 commit 404ff02

1 file changed +5 -0 lines changed

Top

Filter files…

camlibs/ptp2

ptp-pack.c

1 file changed +5 -0 lines changed

Search within code

camlibs/ptp2/ptp-pack.c

```
@@ -881,6 +881,11 @@ ptp_unpack_Sony_DPD (PTPParams *params, const unsigned char* data, PTPDeviceProp
881  881          /* check if we have a secondary list of items, this is for newer Sonys (2024) */
```

```
882  882            if (val < 0x200) {  /* if a secondary list is not provided, this will
                  be the next property code - 0x5XXX or 0xDxxx */
883  883                if (dpd->FormFlag == PTP_DPFF_Enumeration) {
     884  +                 /* free old enum variables */
     885  +                 for (i=0;i<dpd->FORM.Enum.NumberOfValues;i++)
     886  +                     ptp_free_propvalue (dpd->DataType, dpd-
                  >FORM.Enum.SupportedValue+i);
     887  +                 free (dpd->FORM.Enum.SupportedValue);
     888  +
884  889                   N = dtoh16o(data, *poffset);
885  890                   dpd->FORM.Enum.SupportedValue = calloc(N,sizeof(dpd-
                  >FORM.Enum.SupportedValue[0]));
886  891                   if (!dpd->FORM.Enum.SupportedValue)
```

Comments 0

Please sign in to comment.