gphoto / **libgphoto2** Public

Code Issues 441 Pull requests 16 Actions Projects Wiki Sec

Commit 3b9f969

msmeissn committed 3 days ago · ✓ 4 / 4

```
Fixed Sony DPD Enum Count OOB Read (CWE-125) — MEDIUM

In the PTP_DPFF_Enumeration case of ptp_unpack_Sony_DPD(), dtoh16o(data, *poffset) reads 2
bytes for enumeration count N without verifying 2 bytes remain. The standard parser at line
704 has this check.

CVE-2026-40338

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

master

1 parent 433bde9 commit 3b9f969

1 file changed +1 -0 lines changed ↑ Top

Filter files...

camlibs/ptp2

ptp-pack.c

1 file changed +1 -0 lines changed Search within code

camlibs/ptp2/ptp-pack.c

```
@@ -857,6 +857,7 @@ ptp_unpack_Sony_DPD (PTPParams *params, const unsigned
char* data, PTPDeviceProp
857  857            break;
858  858        case PTP_DPFF_Enumeration: {
859  859    #define N   dpd->FORM.Enum.NumberOfValues
     860  +         if (*poffset + sizeof(uint16_t) > dpdlen) goto outofmemory;
860  861            N = dtoh16o(data, *poffset);
```

```
861   862             dpd->FORM.Enum.SupportedValue = calloc(N,sizeof(dpd-
>FORM.Enum.SupportedValue[0]));
862   863             if (!dpd->FORM.Enum.SupportedValue)
```

Comments 0

Please sign in to comment.