gphoto / **libgphoto2** Public

Code Issues 441 Pull requests 16 Actions Projects Wiki Sec

# Commit `09f8a94`

**msmeissn** committed 3 days ago · ✓ 4 / 4

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

ptp_unpack_Sony_DPD() reads the FormFlag byte via dtoh8o(data, *poffset)
without a prior bounds check. The standard ptp_unpack_DPD() at line
686–687 correctly validates *offset + sizeof(uint8_t) > dpdlen before
this same read, but the Sony variant omits this check.

CVE-2026-40339

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

master

1 parent 3b9f969 commit 09f8a94

## 1 file changed +2 -1 lines changed

Top

Filter files…

camlibs/ptp2

ptp-pack.c

## 1 file changed +2 -1 lines changed

Search within code

camlibs/ptp2/ptp-pack.c

```
@@ -839,9 +839,10 @@ ptp_unpack_Sony_DPD (PTPParams *params, const unsigned
char* data, PTPDeviceProp
839 839          code or the Data Type is a string (with two empty strings as
840 840          values). In both cases Form Flag should be set to 0x00 and FORM is
841 841          not present. */
842     -
843 842      if (*poffset==PTP_dpd_Sony_DefaultValue)
844 843          return 1;
```

```
        844 +       if (*poffset + sizeof(uint8_t) > dpdlen)
        845 +           return 1;
845     846
846     847         dpd->FormFlag = dtoh8o(data, *poffset);
847     848         ptp_debug (params, "formflag 0x%04x", dpd->FormFlag);
```

## Comments 0

Please sign in to comment.