gphoto / **libgphoto2** Public

Code | Issues 441 | Pull requests 16 | Actions | Projects | Wiki | Sec

Commit c385b34

msmeissn committed 3 days ago · ✓ 4 / 4

```
Fixed OOB read in ptp_unpack_EOS_FocusInfoEx

Do not read out values before checking there is sufficient size

CVE-2026-40341
```

master

1 parent 404ff02 commit c385b34

1 file changed +25 -9 lines changed

Top

Filter files…

camlibs/ptp2

ptp-pack.c

1 file changed +25 -9 lines changed

Search within code

camlibs/ptp2/ptp-pack.c

```
@@ -1601,23 +1601,39 @@ ptp_pack_EOS_ImageFormat (PTPParams* params,
unsigned char* data, uint16_t value
1601 1601  static inline char*
1602 1602  ptp_unpack_EOS_FocusInfoEx (PTPParams* params, const unsigned char** data,
           uint32_t datasize)
1603 1603  {
1604      -     uint32_t size          = dtoh32a( *data );
1605      -     uint32_t halfsize      = dtoh16a( (*data) + 4);
1606      -     uint32_t version       = dtoh16a( (*data) + 6);
1607      -     uint32_t focus_points_in_struct = dtoh16a( (*data) + 8);
1608      -     uint32_t focus_points_in_use    = dtoh16a( (*data) + 10);
```

```
1609        -     uint32_t sizeX          = dtoh16a( (*data) + 12);
1610        -     uint32_t sizeY          = dtoh16a( (*data) + 14);
1611        -     uint32_t size2X         = dtoh16a( (*data) + 16);
1612        -     uint32_t size2Y         = dtoh16a( (*data) + 18);
            1604  +     uint32_t size;
            1605  +     uint32_t halfsize;
            1606  +     uint32_t version;
            1607  +     uint32_t focus_points_in_struct;
            1608  +     uint32_t focus_points_in_use;
            1609  +     uint32_t sizeX;
            1610  +     uint32_t sizeY;
            1611  +     uint32_t size2X;
            1612  +     uint32_t size2Y;
1613        1613        uint32_t i;
1614        1614        uint32_t maxlen;
1615        1615        char    *str, *p;
1616        1616
            1617  +     if (datasize<4) {
            1618  +         ptp_error(params, "FocusInfoEx has invalid size (%d)", datasize);
            1619  +         return strdup("bad size 0");
            1620  +     }
            1621  +
            1622  +     size            = dtoh32a( *data );
1617        1623        if ((size > datasize) || (size < 20)) {
1618        1624            ptp_error(params, "FocusInfoEx has invalid size (%d) vs datasize
                  (%d)", size, datasize);
1619        1625            return strdup("bad size 1");
1620        1626        }
            1627  +
            1628  +     halfsize        = dtoh16a( (*data) + 4);
            1629  +     version         = dtoh16a( (*data) + 6);
            1630  +     focus_points_in_struct  = dtoh16a( (*data) + 8);
            1631  +     focus_points_in_use = dtoh16a( (*data) + 10);
            1632  +     sizeX           = dtoh16a( (*data) + 12);
            1633  +     sizeY           = dtoh16a( (*data) + 14);
            1634  +     size2X          = dtoh16a( (*data) + 16);
            1635  +     size2Y          = dtoh16a( (*data) + 18);
            1636  +
1621        1637        /* If data is zero-filled, then it is just a placeholder, so nothing
1622        1638           useful, but also not an error */
```

```
1623  1639        if (!focus_points_in_struct || !focus_points_in_use) {
```

Comments 0

Please sign in to comment.