

gphoto / libgphoto2 Public

<> Code Issues 441 Pull requests 16 Actions Projects Wiki Sec

Commit 259fc7d



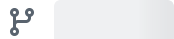
msmeissn committed 3 days ago · ✓ 4 / 4

Fixed Canon FolderEntry Missing Null Termination

ptp_unpack_Canon_FE() copies filename with strncpy into a 13-byte buffer without explicit null termination. The EOS variant at line 1451-1452 correctly adds fe->Filename[PTP_CANON_FilenameBufferLen-1] = 0; confirming this was recognized as necessary but not applied to the original Canon path.

CVE-2026-40334

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



1 parent [7c7f515](#) commit 259fc7d

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

```

@@ -1380,6 +1380,7 @@ ptp_unpack_Canon_FE (PTPParams *params, const
 unsigned char* data, PTPCANONFolde
1380 1380     fe->ObjectSize      = dtoh32a(data + PTP_cfe_ObjectSize);
1381 1381     fe->Time           = (time_t)dtoh32a(data + PTP_cfe_Time);
1382 1382     strncpy(fe->Filename, (char*)data + PTP_cfe_Filename,
        PTP_CANON_FilenameBufferLen);
1383 +     fe->Filename[PTP_CANON_FilenameBufferLen-1] = '\0';

```

```
1383 1384 }  
1384 1385  
1385 1386 /*
```



Comments 0



Please [sign in](#) to comment.