Missing null termination in ptp_unpack_Canon_FE() filename buffer in ptp-pack.c

Low **msmeissn** published **GHSA-ph87-cc3j-c6hm** 3 days ago

Package

libgphoto2

Affected versions

<= 2.5.33

Patched versions

None

Description

Summary

A missing null terminator exists in ptp_unpack_Canon_FE() in camlibs/ptp2/ptp-pack.c (line 1377). The function copies a filename into a 13-byte buffer using strncpy without explicitly null-terminating the result. If the source data is exactly 13 bytes with no null terminator, the buffer is left unterminated, leading to out-of-bounds reads in any subsequent string operation.

Tested against commit `dc49f1b`.

Technical Details

File: camlibs/ptp2/ptp-pack.c, line 1377

Vulnerable Canon path (missing null terminator):
strncpy(fe->Filename,
(char*)data + PTP_cfe_Filename,
PTP_CANON_FilenameBufferLen);

The EOS variant at lines 1451-1452 correctly adds:
fe->Filename[PTP_CANON_FilenameBufferLen-1] = 0;

This confirms the pattern was recognized as necessary but was not applied to the original Canon path. A malicious device sending a 13-byte filename with no null terminator leaves the buffer unterminated.

Suggested Fix

```
strncpy(fe->Filename,
        (char*)data + PTP_cfe_Filename,
        PTP_CANON_FilenameBufferLen);
fe->Filename[PTP_CANON_FilenameBufferLen-1] = '\0';
```

Impact

A malicious Canon USB device can send a crafted folder entry with an unterminated filename, causing subsequent string operations on fe->Filename to read beyond the buffer boundary. CWE-170. Independently fixable from all other findings.

Severity

Low 3.5 / 10

CVSS v3 base metrics

Attack vector	Physical
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

CVE ID

CVE-2026-40334

Weaknesses

▶ CWE-170

Credits

Sebasteuo Reporter