

gphoto / libgphoto2 Public

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

Commit 7c7f515



msmeissn committed 3 days ago · ✓ 4 / 4

Fixed ObjectInfo Parser OOB Read

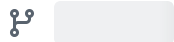
ptp_unpack_OI() validates len < PTP_oi_SequenceNumber (i.e., len < 48) but then accesses:

```
Offsets 48-51: dtoh32a(data + PTP_oi_SequenceNumber) at line 563 (4 bytes OOB)
Offset 52: data[PTP_oi_filenamelen] at line 547 (5 bytes OOB)
Offset 56: data[PTP_oi_filenamelen+4] at line 547 (9 bytes OOB)
```

The Samsung Galaxy 64-bit objectsize detection heuristic reads up to 9 bytes beyond the validated boundary.

CVE-2026-40340

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



1 parent [1817ece](#) commit 7c7f515

1 file changed +1 -1 lines changed

↑ Top

Filter files...

- camlibs/ptp2
 - ptp-pack.c


1 file changed +1 -1 lines changed

Search within code

```

camlibs/ptp2/ptp-pack.c
@@ -532,7 +532,7 @@ ptp_unpack_OI (PTPPParams *params, const unsigned char*
data, PTPObjectInfo *oi,
532 532  {
533 533     char *capture_date;
534 534

```

535	-	<code>if (!data len < PTP_oi_SequenceNumber)</code>
535	+	<code>if (!data len < PTP_oi_filenamelen + 5)</code>
536	536	<code>return;</code>
537	537	
538	538	<code>oi->Filename = oi->Keywords = NULL;</code>
		

Comments 0



Please [sign in](#) to comment.