# Security Advisory 2026-0072

| | |
|---|---|
| **Summary** | Multiple out-of-bounds reads, out-of-bounds writes, and integer overflow vulnerabilities in the AVI demuxer |
| **Date** | 2026-08-05 |
| **Affected Versions** | GStreamer gst-plugins-good < 1.28.6 |
| **IDs** | GStreamer-SA-2026-0072 |

## Details

Multiple vulnerabilities in the AVI demuxer (avidemux) in gst-plugins-good when parsing crafted AVI files.

An unsigned integer underflow in the stream details chunk parser for the FUJIFILM metadata path allows an out-of-bounds heap read and out-of-bounds heap write. The parser decrements a remaining-size counter by fixed offsets without verifying sufficient data remains, causing the counter to wrap to a very large value for undersized chunks. The subsequent null-terminated string scan and byte-level date format modification then read and write far past the end of the allocated buffer.

A related issue in the same function writes to read-only memory-mapped buffer data when performing date format normalization, causing a crash.

An out-of-bounds read in the video properties ODML header parser results from using the user-controlled field count as a divisor instead of the actual field descriptor size when calculating how many entries fit in the buffer. This allows the parser to read beyond the allocated memory.

An out-of-bounds read in the Nikon metadata tag parser dereferences a pointer without first checking that any data remains in the buffer.

Integer overflow vulnerabilities in the superindex and subindex parsers allow an attacker to bypass bounds checks. The bytes-per-entry value multiplied by the loop index overflows, wrapping to a small value that passes the size comparison check, leading to out-of-bounds reads of the mapped buffer.

A missing validation on the entry count in the subindex parser allows an arbitrarily large number of entries to be processed, resulting in excessive memory allocation and denial of service.

## Impact

A malicious third party could trigger a crash of the application by supplying a crafted AVI file, resulting in denial of service. The out-of-bounds read in the FUJIFILM stream details parser has been confirmed to leak adjacent heap memory into parsed tag metadata, which constitutes an information disclosure vulnerability. The out-of-bounds write in the same path could potentially lead to data corruption or arbitrary code execution, although no reliable exploitation was demonstrated. Since the AVI demuxer is auto-plugged by playbin, decodebin, and gst-discoverer pipelines, merely opening or previewing such a file is sufficient to trigger the vulnerabilities.

## Solution

The gst-plugins-good 1.28.6 release addresses the issues. People using older versions of GStreamer should apply the patch and recompile.

## References

### The GStreamer project

- https://gstreamer.freedesktop.org

### CVE Database Entries

- No CVE number assigned or pending

### GStreamer 1.28.6 release

- Release Notes
- GStreamer Plugins Good 1.28.6

### Patches

- Patch

*Report a problem on this page.*