Security Advisory 2026-0075

Summary	Integer overflow and underflow in ASF demuxer bounds checks
Date	2026-08-05
Affected Versions	GStreamer gst-plugins-ugly < 1.28.6
IDs	GStreamer-SA-2026-0075

Details

Multiple integer overflow and underflow vulnerabilities in the ASF demuxer (asfdemux) in gst-plugins-ugly when parsing header objects from crafted ASF, WMV, or WMA files.

The demuxer performs arithmetic on attacker-controlled length and size values read from file headers without sufficient validation. In one case, length fields are summed using 32-bit unsigned arithmetic that can wrap around, causing the resulting value to appear smaller than the individual operands and bypassing the available-data bounds check. In other cases, constants are subtracted from size fields without verifying that the fields are large enough, causing unsigned underflow that produces unexpectedly large values.

Impact

A malicious third party could trigger out-of-bounds reads by providing a crafted ASF, WMV, or WMA file, potentially resulting in application crash, denial of service, or information disclosure. Because the ASF demuxer is auto-plugged by playbin and decodebin, merely opening or previewing a crafted file is sufficient to trigger the vulnerability. The over-read data may also be incorporated into media metadata tags, enabling limited heap information leakage.

Solution

The gst-plugins-ugly 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 Ugly 1.28.6

Patches

- Patch

Report a problem on this page.