



# CVE-2017-5840

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-5840
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-09 15:59:00 UTC
<b>Updated</b>	2020-05-30 18:15:00 UTC
<b>Description</b>	The qtdemux_parse_samples function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gstreamer Project</a>	<a href="#">Gstreamer</a>	All	All	All	All

## References

Reference	Source	Link
GStreamer 1.10 release notes	CONFIRM	<a href="#">gstreamer.freedesktop.org</a>
[SECURITY] [DLA 2225-1] gst-plugins-good0.10 security update	MLIST	<a href="#">lists.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
Bug 777469 – qtdemux: out of bounds heap read in qtdemux_parse_samples	CONFIRM	<a href="#">bugzilla.gnome.org</a>
oss-security - Re: Multiple memory access issues in gstreamer	MLIST	<a href="#">www.openwall.com</a>
Debian -- Security Information -- DSA-3820-1 gst-plugins-good1.0	DEBIAN	<a href="#">www.debian.org</a>
Multiple GStreamer Plug-ins Buffer Overflow and Denial Of Service Vulnerabilities	BID	<a href="#">www.securityfocus.com</a>
GStreamer plug-ins: User-assisted execution of arbitrary code (GLSA 201705-10) — Gentoo Security	GENTOO	<a href="#">security.gentoo.org</a>
oss-security - Multiple memory access issues in gstreamer	MLIST	<a href="#">www.openwall.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[501184](#) Alpine Linux Security Update for gst-plugins-good

[504918](#) Alpine Linux Security Update for gst-plugins-good

[710553](#) Gentoo Linux GStreamer plug-ins User-assisted execution of arbitrary code Vulnerability (GLSA 201705-10)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)