



CVE-2016-9636

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-9636 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-01-27 22:59:00 UTC |
| Updated | 2018-01-05 02:31:00 UTC |
| Description | Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|--|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Gstreamer | Gstreamer | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |

References

| Reference | Source | Link |
|--|---------|--|
| Bug 774834 – flic decoder: Buffer overflow in flx_decode_delta_fli | CONFIRM | bugzilla.gnome.org |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com |
| Debian -- Security Information -- DSA-3724-1 gst-plugins-good0.10 | DEBIAN | www.debian.org |

| | | |
|---|---------|--|
| GStreamer Good Plug-ins Multiple Buffer Overflow Vulnerabilities | BID | www.securityfocus.com |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com |
| GStreamer 1.10 release notes | CONFIRM | gststreamer.freedesktop.org |
| oss-security - Re: CVE Request: gstreamer plugins | MLIST | www.openwall.com |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com |
| GStreamer plug-ins: User-assisted execution of arbitrary code (GLSA 201705-10) — Gentoo Security | GENTOO | security.gentoo.org |
| Security: [0day] [exploit] Advancing exploitation: a scriptless 0day exploit against Linux desktops | MISC | scarybeastsecurity.blogspot |
| Debian -- Security Information -- DSA-3723-1 gst-plugins-good1.0 | DEBIAN | www.debian.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378147](#) Virtuozzo Linux Security Update for gstreamer-plugins-good (VZLSA-2017:0019)

[378149](#) Virtuozzo Linux Security Update for gstreamer1-plugins-good (VZLSA-2017:0020)

[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