



CVE-2017-5884

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

Summary

CVE	CVE-2017-5884
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-28 18:59:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	gtk-vnc before 0.7.0 does not properly check boundaries of subrectangle-containing tiles, which allows remote servers to e

Risk And Classification

Problem Types: CWE-118

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Application	Gnome	Gtk-vnc	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 25 Update: gtk-vnc-0.7.0-1.fc25 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
[SECURITY] Fedora 25 Update: gtk-vnc-0.7.0-1.fc25 - package-announce - Fedora Mailing-Lists	MISC	lists.f
oss-security - Re: CVE request for two input validation flaws in gtk-vnc	MLIST	www.
1418944 – (CVE-2017-5884) CVE-2017-5884 gtk-vnc: Improper check of framebuffer boundaries when processing a tile	MISC	bugzi
gtk-vnc Remote Code Execution Vulnerability and Multiple Integer Overflow Vulnerabilities	BID	www.
oss-security - CVE request for two input validation flaws in gtk-vnc	MLIST	www.
CVE-2017-5884 - Red Hat Customer Portal	MISC	acce
Red Hat Customer Portal	REDHAT	acce
Bug 778048 – The code does not check framebuffer boundaries sufficiently when processing a tile	CONFIRM	bugzi
gtk-vnc - A VNC viewer widget for GTK+	CONFIRM	git.gn
CVE Program record	CVE.ORG	www.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500993](#) Alpine Linux Security Update for gtk-vnc

[504921](#) Alpine Linux Security Update for gtk-vnc

[751144](#) SUSE Enterprise Linux Security Update for gtk-vnc (SUSE-SU-2021:3125-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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