



# CVE-2016-10207

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

## Summary

<b>CVE</b>	CVE-2016-10207
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-28 18:59:00 UTC
<b>Updated</b>	2018-02-01 17:05:00 UTC
<b>Description</b>	The Xvnc server in TigerVNC allows remote attackers to cause a denial of service (invalid memory access and crash) by te

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	0.0.90	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	0.0.91	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.0	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.0.1	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.1.0	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.3	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.3.1	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.7	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	0.0.90	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	0.0.91	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.0	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.0.1	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.1.0	All	All	All

Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.3	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.3.1	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	1.7	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
TigerVNC: Multiple vulnerabilities (GLSA 201801-13) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
oss-security - CVE request tigervnc: vnc server can crash when TLS handshake terminates early	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
TigerVNC CVE-2016-10207 Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
[security-announce] openSUSE-SU-2017:0444-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Proper global init/deinit of GnuTLS · TigerVNC/tigervnc@8aa4bc5 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
oss-security - Re: CVE request tigervnc: vnc server can crash when TLS handshake terminates early	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
Bug 1023012 – VUL-0: CVE-2016-10207: tigervnc: crash when TLS handshake terminates early	CONFIRM	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710213](#) Gentoo Linux TigerVNC Multiple Vulnerabilities (GLSA 201801-13)

© [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](https://status.cve.report)