



CVE-2016-4414

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

Summary

CVE	CVE-2016-4414
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-13 19:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The onReadyRead function in core/coreauthhandler.cpp in Quassel before 0.12.4 allows remote attackers to cause a denial of service (CPU consumption) via a long handshake.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Quassel-irc	Quassel	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 22 Update: quassel-0.12.4-1.fc22	FEDORA	lists.fedoraproject.org	
oss-security - Re: CVE request - Quassel IRC denial of service	MLIST	www.openwall.com	
Handle invalid handshake data properly in the core · quassel/quassel@e678873 · GitHub	CONFIRM	github.com	Vendor Advi

openSUSE-SU-2016:1314-1: moderate: Security update for quassel	SUSE	lists.opensuse.org	
[SECURITY] Fedora 23 Update: quassel-0.12.4-1.fc23	FEDORA	lists.fedoraproject.org	
Fixing Bugs - Quassel 0.12.4 Quassel IRC	CONFIRM	quassel-irc.org	
[SECURITY] Fedora 24 Update: quassel-0.12.4-1.fc24	FEDORA	lists.fedoraproject.org	
oss-security - CVE request - Quassel IRC denial of service	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

CVE.report and Source URL Uptime Status status.cve.report