



CVE-2015-8547

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-8547
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-08 19:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The CoreUserInputHandler::doMode function in core/coreuserinputhandler.cpp in Quassel 0.10.0 allows remote attackers to

Risk And Classification

Problem Types: CWE-17

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Quassel-irc	Quassel	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 22 Update: quassel-0.12.2-6.fc22	FEDORA	lists.fedoraproject.org
openSUSE-SU-2015:2345-1: moderate: Security update for quassel	SUSE	lists.opensuse.org
[SECURITY] Fedora 23 Update: quassel-0.12.2-6.fc23	FEDORA	lists.fedoraproject.org
oss-security - Re: CVE request: Remote DoS in Quassel	MLIST	www.openvulnerability.com
Fixes a crash of the core when executing "/op *" in a query. by elxa · Pull Request #153 · quassel/quassel · GitHub	CONFIRM	github.com
Merge pull request #153 from elxa/fix-op-command-crashing-core · quassel/quassel@b8edbdba · GitHub	CONFIRM	github.com
oss-security - CVE request: Remote DoS in Quassel	MLIST	www.openvulnerability.com

CVE Program record

CVE.ORG www.cve.org

NVD vulnerability detail

NVD nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© 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