



CVE-2009-1572

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

Summary

CVE	CVE-2009-1572
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-06 17:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	The BGP daemon (bgpd) in Quagga 0.99.11 and earlier allows remote attackers to cause a denial of service (crash) via an

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quagga	Quagga	0.95	All	All	All
Application	Quagga	Quagga	0.96	All	All	All
Application	Quagga	Quagga	0.96.1	All	All	All
Application	Quagga	Quagga	0.96.2	All	All	All
Application	Quagga	Quagga	0.96.3	All	All	All
Application	Quagga	Quagga	0.96.4	All	All	All
Application	Quagga	Quagga	0.96.5	All	All	All
Application	Quagga	Quagga	0.97.0	All	All	All
Application	Quagga	Quagga	0.97.1	All	All	All
Application	Quagga	Quagga	0.97.2	All	All	All
Application	Quagga	Quagga	0.97.3	All	All	All
Application	Quagga	Quagga	0.97.4	All	All	All
Application	Quagga	Quagga	0.97.5	All	All	All
Application	Quagga	Quagga	0.98.0	All	All	All
Application	Quagga	Quagga	0.98.1	All	All	All
Application	Quagga	Quagga	0.98.2	All	All	All
Application	Quagga	Quagga	0.98.3	All	All	All

Application	Quagga	Quagga	0.98.4	All	All	All
Application	Quagga	Quagga	0.98.5	All	All	All
Application	Quagga	Quagga	0.98.6	All	All	All
Application	Quagga	Quagga	0.99.1	All	All	All
Application	Quagga	Quagga	0.99.10	All	All	All
Application	Quagga	Quagga	0.99.2	All	All	All
Application	Quagga	Quagga	0.99.3	All	All	All
Application	Quagga	Quagga	0.99.4	All	All	All
Application	Quagga	Quagga	0.99.5	All	All	All
Application	Quagga	Quagga	0.99.6	All	All	All
Application	Quagga	Quagga	0.99.7	All	All	All
Application	Quagga	Quagga	0.99.8	All	All	All
Application	Quagga	Quagga	0.99.9	All	All	All
Application	Quagga	Quagga	All	All	All	All
Application	Quagga	Quagga	0.95	All	All	All
Application	Quagga	Quagga	0.96	All	All	All
Application	Quagga	Quagga	0.96.1	All	All	All
Application	Quagga	Quagga	0.96.2	All	All	All
Application	Quagga	Quagga	0.96.3	All	All	All
Application	Quagga	Quagga	0.96.4	All	All	All
Application	Quagga	Quagga	0.96.5	All	All	All
Application	Quagga	Quagga	0.97.0	All	All	All
Application	Quagga	Quagga	0.97.1	All	All	All
Application	Quagga	Quagga	0.97.2	All	All	All
Application	Quagga	Quagga	0.97.3	All	All	All
Application	Quagga	Quagga	0.97.4	All	All	All
Application	Quagga	Quagga	0.97.5	All	All	All
Application	Quagga	Quagga	0.98.0	All	All	All
Application	Quagga	Quagga	0.98.1	All	All	All
Application	Quagga	Quagga	0.98.2	All	All	All
Application	Quagga	Quagga	0.98.3	All	All	All
Application	Quagga	Quagga	0.98.4	All	All	All
Application	Quagga	Quagga	0.98.5	All	All	All
Application	Quagga	Quagga	0.98.6	All	All	All
Application	Quagga	Quagga	0.99.1	All	All	All

Application	Quagga	Quagga	0.99.10	All	All	All
Application	Quagga	Quagga	0.99.2	All	All	All
Application	Quagga	Quagga	0.99.3	All	All	All
Application	Quagga	Quagga	0.99.4	All	All	All
Application	Quagga	Quagga	0.99.5	All	All	All
Application	Quagga	Quagga	0.99.6	All	All	All
Application	Quagga	Quagga	0.99.7	All	All	All
Application	Quagga	Quagga	0.99.8	All	All	All
Application	Quagga	Quagga	0.99.9	All	All	All

References						
Reference			Source		Link	
Security Advisory SA34999 - Debian update for quagga - Secunia			SECUNIA		secunia.com	
Quagga Autonomous System Number Remote Denial Of Service Vulnerability			BID		www.securityfocus.	
54200			OSVDB		www.osvdb.org	
[SECURITY] Fedora 11 Update: quagga-0.99.12-1.fc11			FEDORA		www.redhat.com	
'[quagga-dev 6391] [PATCH] BGP 4-byte ASN bug fixes' - MARC			MLIST		marc.info	
IBM X-Force Exchange			XF		exchange.xforce.ib	
[SECURITY] Fedora 10 Update: quagga-0.99.12-1.fc10			FEDORA		www.redhat.com	
Gmane Loom			MISC		thread.gmane.org	
Support / Security / Advisories // MDVSA-2009:109 Mandriva			MANDRIVA		www.mandriva.com	
USN-775-1: Quagga vulnerability Ubuntu			UBUNTU		www.ubuntu.com	
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com			SECUNIA		secunia.com	
Fedora update for quagga - Secunia Advisories - Vulnerability Information - Secunia.com			SECUNIA		secunia.com	
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012			SUSE		lists.opensuse.org	
Ubuntu update for quagga - Secunia Advisories - Vulnerability Information - Secunia.com			SECUNIA		secunia.com	
Debian -- Security Information -- DSA-1788-1 quagga			DEBIAN		www.debian.org	
Quagga Bug in Processing Certain 4-Byte ASN Data Lets Remote Users Deny Service - SecurityTracker			SECTRACK		www.securitytracke	
oss-security - Re: CVE request (sort of): Quagga BGP crasher			MLIST		www.openwall.com	
oss-security - CVE request (sort of): Quagga BGP crasher			MLIST		www.openwall.com	
#526311 - quagga: bgpd crashes - Debian Bug report logs			CONFIRM		bugs.debian.org	
CVE Program record			CVE.ORG		www.cve.org	
NVD vulnerability detail			NVD		nvd.nist.gov	

Vendor Comments And Credit			
Organization	Published	Contributor	Statement

Red Hat 2009-05-18 Tomas Hoger Not vulnerable. This issue did not affect the versions of zebra as shipped with Red Hat Enterprise Linux 5.4.

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](#).

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

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