CVE-2010-2948

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-2948
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-10 19:00:00 UTC
Updated	2023-02-13 04:21:00 UTC
Description	Stack-based buffer overflow in the bgp_route_refresh_receive function in bgp_packet.c in bgpd in Quagga before 0.99.17 a

Risk And Classification

Problem Types: CWE-119

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	0.99.11	All	All	All
Application	Quagga	Quagga	0.99.12	All	All	All
Application	Quagga	Quagga	0.99.13	All	All	All
Application	Quagga	Quagga	0.99.14	All	All	All
Application	Quagga	Quagga	0.99.15	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	0.99.11	All	All	All
Application	Quagga	Quagga	0.99.12	All	All	All
Application	Quagga	Quagga	0.99.13	All	All	All
Application	Quagga	Quagga	0.99.14	All	All	All
Application	Quagga	Quagga	0.99.15	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
Quagga bgpd Route-Refresh Message Stack Buffer Overflow Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Debian -- Security Information -- DSA-2104-1 quagga
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
USN-1027-1: Quagga vulnerabilities | Ubuntu
Gentoo Linux Documentation -- Quagga: Multiple vulnerabilities
Bug 626783 – CVE-2010-2948 Quagga (bgpd): Stack buffer overflow by processing certain Route-Refresh messages
Support
Support
Quagga BGP Daemon Denial of Service and Buffer Overflow Vulnerabilities - Advisories - Community
Security Advisory SA48106 - Gentoo update for quagga - Secunia
code.quagga.net Git - quagga.git/commit
Support / Security / Advisories / / MDVSA-2010:174 | Mandriva
Quagga Software Routing Suite

Red Hat Customer Portal
Red Hat Customer Portal
SUSE Update for Multiple Packages - Secunia.com
oss-security - Re: CVE Request -- Quagga (bgpd) [two ids] -- 1, Stack buffer overflow by processing crafted Refresh-Route msgs 2, NULL ptr
[security-announce] SUSE-SU-2011:1316-1: important: Security update for
Ubuntu update for quagga - Secunia.com
Red Hat update for quagga - Advisories - Community
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:022
oss-security - CVE Request -- Quagga (bgpd) [two ids] -- 1, Stack buffer overflow by processing crafted Refresh-Route msgs 2, NULL ptr dere
Debian update for quagga - Advisories - Community
access.redhat.com | CVE-2010-2948
code.quagga.net Git - quagga.git/commit
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE Program record
NVD vulnerability detail

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 registred 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**