



CVE-2012-3411

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

Summary

CVE	CVE-2012-3411
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-03-05 21:38:00 UTC
Updated	2023-02-13 00:25:00 UTC
Description	Dnsmasq before 2.63test1, when used with certain libvirt configurations, replies to requests from prohibited interfaces, which

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Thekelleys	Dnsmasq	All	All	All	All

References

Reference
thekelleys.org.uk Git - dnsmasq.git/commitdiff
Red Hat Customer Portal
oss-security - Re: Re: CVE Request -- dnsmasq: When being run by libvirt open DNS proxy (reachable out-of the virtual network set for the pa
Red Hat Customer Portal
thekelleys.org.uk Git - dnsmasq.git/commitdiff
#683372 - CVE-2012-3411: libvirt-controlled dnsmasq replies to DNS queries from non-virtual networks - Debian Bug report logs
thekelleys.org.uk Git - dnsmasq.git/commitdiff

[thekelleys.org.uk Git - dnsmasq.git/commitdiff](https://thekelleys.org.uk/Git-dnsmasq.git/commitdiff)

Bug 833033 – CVE-2012-3411 libvirt+dnsmasq: DNS configured to answer DNS queries from non-virtual networks

Support / Security / Advisories // MDVSA-2013:072 | Mandriva

Red Hat Customer Portal

Dnsmasq Remote Denial of Service Vulnerability

www.thekelleys.org.uk/dnsmasq/CHANGELOG

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](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](#).

Free CVE JSON API cve.report/api

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