



# CVE-2020-25684

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

## Summary

<b>CVE</b>	CVE-2020-25684
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-20 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the for

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Arista</a>	<a href="#">Eos</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Thekelleys</a>	<a href="#">Dnsmasq</a>	All	All	All	All
Application	<a href="#">Thekelleys</a>	<a href="#">Dnsmasq</a>	All	All	All	All

## References

### Reference

[SECURITY] Fedora 33 Update: dnsmasq-2.83-1.fc33 - package-announce - Fedora Mailing-Lists

Security Advisory 0061 - Arista

[SECURITY] [DLA 2604-1] dnsmasq security update

[SECURITY] Fedora 32 Update: dnsmasq-2.84-1.fc32 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 33 Update: dnsmasq-2.83-1.fc33 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 32 Update: dnsmasq-2.84-1.fc32 - package-announce - Fedora Mailing-Lists

1889686 – (CVE-2020-25684) CVE-2020-25684 dnsmasq: loose address/port check in reply\_query() makes forging replies easier for an off-p

Dnsmasq: Multiple vulnerabilities (GLSA 202101-17) — Gentoo security

DNSPOOQ - JSOF

Debian -- Security Information -- DSA-4844-1 dnsmasq

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[178499](#) Debian Security Update for dnsmasq (DLA 2604-1)

[296069](#) Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)

[352293](#) Amazon Linux Security Update for dnsmasq: AL2012-2021-334

[377140](#) Alibaba Cloud Linux Security Update for dnsmasq (ALINUX3-SA-2021:0009)

[377442](#) Alibaba Cloud Linux Security Update for dnsmasq (ALINUX2-SA-2021:0002)

[43821](#) Arista EOS Domain Name System (DNS) cache poisoning Vulnerability (SA0061)

[500150](#) Alpine Linux Security Update for dnsmasq

[503800](#) Alpine Linux Security Update for dnsmasq

[670173](#) EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1673)

[670301](#) EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1775)

[690442](#) Free Berkeley Software Distribution (FreeBSD) Security Update for dnsmasq (5b5cf6e5-5b51-11eb-95ac-7f9491278677)

[730121](#) McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)

[750407](#) OpenSUSE Security Update for dnsmasq (openSUSE-SU-2021:0129-1)

[750409](#) OpenSUSE Security Update for dnsmasq (openSUSE-SU-2021:0124-1)

[900068](#) CBL-Mariner Linux Security Update for dnsmasq 2.79

[903703](#) Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3814)

[940396](#) AlmaLinux Security Update for dnsmasq (ALSA-2021:0150)

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](#)**