



CVE-2022-0934

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

Summary

CVE	CVE-2022-0934
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 15:15:00 UTC
Updated	2023-03-07 18:12:00 UTC
Description	A single-byte, non-arbitrary write/use-after-free flaw was found in dnsmasq. This flaw allows an attacker who sends a crafted

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Thekelleys	Dnsmasq	All	All	All	All
Application	Thekelleys	Dnsmasq	-	All	All	All

References

Reference	Source	Link	Tags
2057075 – (CVE-2022-0934) CVE-2022-0934 dnsmasq: Heap use after free in dhcp6_no_relay	MISC	bugzilla.redhat.com	
thekelleys.org.uk Git - dnsmasq.git/commit	MISC	thekelleys.org.uk	
thekelleys.org.uk Git - dnsmasq.git/commit	MISC	thekelleys.org.uk	
[Dnsmasq-discuss] [PATCH] Heap use after free in dhcp6_no_relay (CVE-2022-0934)	MISC	lists.thekelleys.org.uk	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160216 Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2022-7633)
160296 Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2022-8070)
161016 Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2023-12946)
161022 Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2023-12945)
184671 Debian Security Update for dnsmasq (CVE-2022-0934)
198778 Ubuntu Security Notification for Dnsmasq Vulnerability (USN-5408-1)
240846 Red Hat Update for dnsmasq (RHSA-2022:7633)
240899 Red Hat Update for dnsmasq (RHSA-2022:8070)
243150 Red Hat Update for dnsmasq (RHSA-2024:1545)
354515 Amazon Linux Security Advisory for dnsmasq : ALAS2022-2022-227
354552 Amazon Linux Security Advisory for dnsmasq : ALAS-2022-227
355126 Amazon Linux Security Advisory for dnsmasq : ALAS2023-2023-039
378050 Alibaba Cloud Linux Security Update for dnsmasq (ALINUX3-SA-2023:0024)
378621 Alibaba Cloud Linux Security Update for dnsmasq (ALINUX2-SA-2023:0029)
501955 Alpine Linux Security Update for dnsmasq
503893 Alpine Linux Security Update for dnsmasq
671656 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-1713)
671893 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-1925)
671920 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-1962)
671926 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-1992)
672027 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-2252)
672062 EulerOS Security Update for dnsmasq (EulerOS-SA-2022-2239)
690826 Free Berkeley Software Distribution (FreeBSD) Security Update for dnsmasq (3f321a5a-b33b-11ec-80c2-1bb2c6a00592)
752059 SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2022:1288-1)
752062 SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2022:1289-1)
752067 SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2022:1307-1)

753098 SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2022:14941-1)
905733 Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (25315)
905734 Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (25317)
906684 Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (25317-3)
940768 AlmaLinux Security Update for dnsmasq (ALSA-2022:7633)
940821 AlmaLinux Security Update for dnsmasq (ALSA-2022:8070)
960395 Rocky Linux Security Update for dnsmasq (RLSA-2022:7633)
960586 Rocky Linux Security Update for dnsmasq (RLSA-2022:8070)

© [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](#)