



CVE-2017-14493

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

Summary

CVE	CVE-2017-14493
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-03 01:29:00 UTC
Updated	2023-11-07 02:39:00 UTC
Description	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.1	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.1	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Thekelleys	Dnsmasq	All	All	All	All

References

Reference

thekelleys.org.uk/dnsmasq/CHANGELOG

Debian -- Security Information -- DSA-3989-1 dnsmasq

Vulnerability Note VU#973527 - Dnsmasq contains multiple vulnerabilities

Security Bulletin: NVIDIA Tegra Jetson L4T contains multiple vulnerabilities; updates for "BlueBorne" and "Dnsmasq". | NVIDIA

Dnsmasq Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Obtain Potentially Sensitive Information - SecurityTrac

USN-3430-2: Dnsmasq vulnerabilities | Ubuntu

Dnsmasq: Multiple vulnerabilities (GLSA 201710-27) — Gentoo security

Synology-SA-17:59 Dnsmasq | Synology Inc.

www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-005.txt

Red Hat Customer Portal

dnsmasq: Multiple Critical and Important vulnerabilities - Red Hat Customer Portal

USN-3430-1: Dnsmasq vulnerabilities | Ubuntu

Dnsmasq < 2.78 - Stack-Based Overflow

thekelleys.org.uk Git - dnsmasq.git/commit

Dnsmasq VU#973527 Multiple Security Vulnerabilities

[Dnsmasq-discuss] IMPORTANT SECURITY INFORMATION.

Google Online Security Blog: Behind the Masq: Yet more DNS, and DHCP, vulnerabilities

[Dnsmasq-discuss] Announce: dnsmasq-2.78.

[security-announce] openSUSE-SU-2017:2633-1: important: Security update

Red Hat Customer Portal

[Dnsmasq-discuss] IMPORTANT SECURITY INFORMATION.

thekelleys.org.uk Git - dnsmasq.git/commit

[Dnsmasq-discuss] Announce: dnsmasq-2.78.

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500147](#) Alpine Linux Security Update for dnsmasq

[503797](#) Alpine Linux Security Update for dnsmasq

[710376](#) Gentoo Linux Dnsmasq Multiple Vulnerabilities (GLSA 201710-27)

© [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](#)