CVE-2017-14496

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-14496
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	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-su

Risk And Classification

Problem Types: CWE-191

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	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All

Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Novell	Leap	42.2	All	All	All
Operating System	Novell	Leap	42.3	All	All	All
Operating System	Novell	Leap	42.2	All	All	All
Operating System	Novell	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
Dnsmasq < 2.78 - Integer Underflow
thekelleys.org.uk/dnsmasq/CHANGELOG
Debian -- Security Information -- DSA-3989-1 dnsmasq
thekelleys.org.uk Git - dnsmasq.git/commit
Vulnerability Note VU#973527 - Dnsmasq contains multiple vulnerabilities
RETIRED: Multiple Siemens SCALANCE Products Multiple Security 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

Android Security Bulletin—October 2017 | Android Open Source Project
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
cert-portal.siemens.com/productcert/pdf/ssa-689071.pdf
Red Hat Customer Portal
dnsmasq: Multiple Critical and Important vulnerabilities - Red Hat Customer Portal
thekelleys.org.uk Git - dnsmasq.git/commit
USN-3430-1: Dnsmasq vulnerabilities | Ubuntu
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
[Dnsmasq-discuss] IMPORTANT SECURITY INFORMATION.
[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)