CVE-2017-14491

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-14491
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-04 01:29:00 UTC
Updated	2023-11-07 02:39:00 UTC
Description	Heap-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-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arista	Eos	All	All	All	All
Operating System	Arista	Eos	All	All	All	All
Operating System	Arista	Eos	All	All	All	All
Operating System	Arubanetworks	Arubaos	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	12.04	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	8.0	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
Hardware	Huawei	Honor V9 Play	-	All	All	All
Operating System	Huawei	Honor V9 Play Firmware	All	All	All	All
Operating System	Microsoft	Windows	-	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
Application	Nvidia	Geforce Experience	All	All	All	All
Hardware	Nvidia	Jetson Tk1	-	All	All	All
Hardware	Nvidia	Jetson Tx1	-	All	All	All
Operating System	Nvidia	Linux For Tegra	All	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Hardware	Siemens	Ruggedcom Rm1224	-	All	All	All
Operating System	Siemens	Ruggedcom Rm1224 Firmware	All	All	All	All
Hardware	Siemens	Scalance M-800	-	All	All	All
Operating System	Siemens	Scalance M-800 Firmware	All	All	All	All
Hardware	Siemens	Scalance S615	-	All	All	All
Operating System	Siemens	Scalance S615 Firmware	All	All	All	All
Hardware	Siemens	Scalance W1750d	-	All	All	All

Operating System	Siemens	Scalance W1750d Firmware	All	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Application	Suse	Linux Enterprise Point Of Sale	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Application	Synology	Diskstation Manager	5.2	All	All	All
Application	Synology	Diskstation Manager	6.0	All	All	All
Application	Synology	Diskstation Manager	6.1	All	All	All
Application	Synology	Router Manager	1.1	All	All	All
Application	Thekelleys	Dnsmasq	All	All	All	All

References

Reference
thekelleys.org.uk Git - dnsmasq.git/commit
Red Hat Customer Portal
BSA-2017-449
thekelleys.org.uk/dnsmasq/CHANGELOG
Debian -- Security Information -- DSA-3989-1 dnsmasq
[security-announce] SUSE-SU-2017:2619-1: important: Security update for dnsmasq - openSUSE Security Announce - openSUSE Mailing Lis
Vulnerability Note VU#973527 - Dnsmasq contains multiple vulnerabilities
[SECURITY] Fedora 27 Update: dnsmasq-2.77-9.fc27 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
RETIRED: Multiple Siemens SCALANCE Products Multiple Security Vulnerabilities
Security Bulletin: NVIDIA Tegra Jetson L4T contains multiple vulnerabilities; updates for “BlueBorne” and “Dnsmasq”. | NVIDIA
Security Advisory 0030 - Arista
thekelleys.org.uk Git - dnsmasq.git/commit
Red Hat Customer Portal
Dnsmasq Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Obtain Potentially Sensitive Information - SecurityTrac
[security-announce] SUSE-SU-2017:2617-1: important: Security update for dnsmasq - openSUSE Security Announce - openSUSE Mailing Lis
USN-3430-2: Dnsmasq vulnerabilities | Ubuntu
Dnsmasq 2-Byte Heap-Based Overflow ≈ Packet Storm
Debian -- Security Information -- DSA-3989-1 dnsmasq
Red Hat Customer Portal
Dnsmasq: Multiple vulnerabilities (GLSA 201710-27) — Gentoo security

Synology-SA-17:59 Dnsmasq | Synology Inc.
[SECURITY] Fedora 25 Update: dnsmasq-2.76-4.fc25 - package-announce - Fedora Mailing-Lists
[security-announce] SUSE-SU-2017:2616-1: important: Security update for dnsmasq - openSUSE Security Announce - openSUSE Mailing Lis
www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-005.txt
Security Bulletin: NVIDIA Installer Framework contains a vulnerability in NVISystemService64 affecting GFE | NVIDIA
Dnsmasq < 2.78 - 2-byte Heap Overflow
USN-3430-3: Dnsmasq regression | Ubuntu
cert-portal.siemens.com/productcert/pdf/ssa-689071.pdf
BSA-2017-449
Red Hat Customer Portal
[SECURITY] Fedora 25 Update: dnsmasq-2.76-4.fc25 - package-announce - Fedora Mailing-Lists
dnsmasq: Multiple Critical and Important vulnerabilities - Red Hat Customer Portal
USN-3430-1: Dnsmasq vulnerabilities | Ubuntu
[SECURITY] Fedora 26 Update: dnsmasq-2.76-5.fc26 - package-announce - Fedora Mailing-Lists
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 Advisory - Seven vulnerabilities in Google Dnsmasq
[security-announce] openSUSE-SU-2017:2633-1: important: Security update
Red Hat Customer Portal
[SECURITY] Fedora 26 Update: dnsmasq-2.76-5.fc26 - package-announce - Fedora Mailing-Lists
[Dnsmasq-discuss] IMPORTANT SECURITY INFORMATION.
[SECURITY] Fedora 27 Update: dnsmasq-2.77-9.fc27 - package-announce - Fedora Mailing-Lists
[Dnsmasq-discuss] Announce: dnsmasq-2.78.
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

352293 Amazon Linux Security Update for dnsmasq: AL2012-2021-334

378236 Virtuozzo Linux Security Update for dnsmasq-utils (VZLSA-2017:2838)

500147 Alpine Linux Security Update for dnsmasq

503797 Alpine Linux Security Update for dnsmasq

610322 Google Android Devices March 2021 Security Patch Missing

610323 Google Android March 2021 Security Patch Missing for LGE

610324 Google Android March 2021 Security Patch Missing for Huawei EMUI

610325 Google Android March 2021 Security Patch Missing for Samsung

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