CVE-2020-25685

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25685
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-20 16:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forwar

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arista	Eos	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Thekelleys	Dnsmasq	All	All	All	All
Application	Thekelleys	Dnsmasq	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] 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

Dnsmasq: Multiple vulnerabilities (GLSA 202101-17) — Gentoo security
DNSPOOQ - JSOF
1889688 – (CVE-2020-25685) CVE-2020-25685 dnsmasq: loose query name check in reply_query() makes forging replies easier for an off-pa
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

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
903378	Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3816)
940396	AlmaLinux Security Update for dnsmasq (ALSA-2021:0150)

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report