



CVE-2023-50387

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

Summary

CVE	CVE-2023-50387
State	PUBLISHED
Assigner	Unknown
Source Priority	Enrichment-only fallback
Published	Unknown
Updated	Unknown
Description	Description unavailable.

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [15154](#) ISC BIND Extreme CPU consumption Vulnerability (CVE-2023-50387)
- [161387](#) Oracle Enterprise Linux Security Update for unbound (ELSA-2024-0977)
- [161388](#) Oracle Enterprise Linux Security Update for unbound (ELSA-2024-0965)
- [161414](#) Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2024-1335)
- [161416](#) Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2024-1334)
- [161481](#) Oracle Enterprise Linux Security Update for bind and dhcp (ELSA-2024-1782)
- [161482](#) Oracle Enterprise Linux Security Update for bind9.16 (ELSA-2024-1781)
- [161484](#) Oracle Enterprise Linux Security Update for bind (ELSA-2024-1789)
- [200108](#) Ubuntu Security Notification for Bind Vulnerabilities (USN-6633-1)
- [200121](#) Ubuntu Security Notification for Bind Vulnerabilities (USN-6642-1)

200141 Ubuntu Security Notification for Dnsmasq Vulnerabilities (USN-6657-1)
200154 Ubuntu Security Notification for Unbound Vulnerabilities (USN-6665-1)
200245 Ubuntu Security Notification for Bind Vulnerabilities (USN-6723-1)
242950 Red Hat Update for unbound (RHSA-2024:0982)
242958 Red Hat Update for unbound (RHSA-2024:0977)
242960 Red Hat Update for unbound (RHSA-2024:0981)
242976 Red Hat Update for unbound (RHSA-2024:0965)
243072 Red Hat Update for dnsmasq (RHSA-2024:1334)
243073 Red Hat Update for dnsmasq (RHSA-2024:1335)
243136 Red Hat Update for dnsmasq (RHSA-2024:1522)
243146 Red Hat Update for dnsmasq (RHSA-2024:1544)
243149 Red Hat Update for dnsmasq (RHSA-2024:1543)
243150 Red Hat Update for dnsmasq (RHSA-2024:1545)
243161 Red Hat Update for bind9.16 (RHSA-2024:1647)
243168 Red Hat Update for bind9.16 (RHSA-2024:1648)
243186 Red Hat Update for bind9.16 (RHSA-2024:1781)
243187 Red Hat Update for bind and dhcp (RHSA-2024:1782)
243190 Red Hat Update for bind (RHSA-2024:1789)
284930 Fedora Security Update for pdns (FEDORA-2024-4e36df9dfd)
284937 Fedora Security Update for bind9 (FEDORA-2024-c36c448396)
284945 Fedora Security Update for unbound (FEDORA-2024-c967c7d287)
284946 Fedora Security Update for dnsmasq (FEDORA-2024-e00eceb11c)
284952 Fedora Security Update for bind (FEDORA-2024-fae88b73eb)
284970 Fedora Security Update for bind (FEDORA-2024-21310568fa)
284971 Fedora Security Update for bind9 (FEDORA-2024-499b9be35f)
284979 Fedora Security Update for unbound (FEDORA-2024-2e26eccfcb)
284980 Fedora Security Update for pdns (FEDORA-2024-b0f9656a76)
284982 Fedora Security Update for dnsmasq (FEDORA-2024-e24211eff0)
357276 Amazon Linux Security Advisory for unbound : ALAS2-2024-2481

357286 Amazon Linux Security Advisory for bind : ALAS2023-2024-550
357292 Amazon Linux Security Advisory for dnsmasq : ALAS2023-2024-552
357294 Amazon Linux Security Advisory for unbound : ALAS2023-2024-553
379639 Alibaba Cloud Linux Security Update for unbound (ALINUX3-SA-2024:0027)
510730 Alpine Linux Security Update for bind
510731 Alpine Linux Security Update for bind
510732 Alpine Linux Security Update for dnsmasq
510734 Alpine Linux Security Update for pdns-recursor
510735 Alpine Linux Security Update for unbound
510737 Alpine Linux Security Update for knot-resolver
510739 Alpine Linux Security Update for knot-resolver
510740 Alpine Linux Security Update for unbound
510742 Alpine Linux Security Update for dnsmasq
6000474 Debian Security Update for unbound (DSA 5620-1)
6000475 Debian Security Update for bind9 (DSA 5621-1)
6000481 Debian Security Update for pdns-recursor (DSA 5626-1)
6000483 Debian Security Update for unbound (DLA 3736-1)
6000496 Debian Security Update for knot-resolver (DSA 5633-1)
674119 EulerOS Security Update for unbound (EulerOS-SA-2024-1500)
674123 EulerOS Security Update for bind (EulerOS-SA-2024-1502)
674132 EulerOS Security Update for bind (EulerOS-SA-2024-1481)
674154 EulerOS Security Update for unbound (EulerOS-SA-2024-1521)
691427 Free Berkeley Software Distribution (FreeBSD) Security Update for dnssec validators (21a854cc-cac1-11ee-b7a7-353f1e043d9a)
691430 Free Berkeley Software Distribution (FreeBSD) Security Update for powerdns (e15ba624-cca8-11ee-84ca-b42e991fc52e)
755824 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2024:0590-1)
908005 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (34350-1)
908016 Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (34419-1)
908017 Common Base Linux Mariner (CBL-Mariner) Security Update for unbound (34440-1)

92116 Microsoft Windows Domain Name System (DNS) Server Denial of Service (DoS) Vulnerability for February 2024
941593 AlmaLinux Security Update for unbound (ALSA-2024:0965)
941600 AlmaLinux Security Update for unbound (ALSA-2024:0977)
941622 AlmaLinux Security Update for dnsmasq (ALSA-2024:1335)
941623 AlmaLinux Security Update for dnsmasq (ALSA-2024:1334)
941656 AlmaLinux Security Update for bind and dhcp (ALSA-2024:1782)
941658 AlmaLinux Security Update for bind9.16 (ALSA-2024:1781)
941663 AlmaLinux Security Update for bind (ALSA-2024:1789)
961137 Rocky Linux Security Update for dnsmasq (RLSA-2024:1335)

© [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](#)