



CVE-2008-3214

Published on: 07/18/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:12 PM UTC

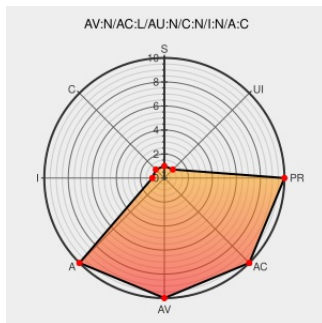
CVE-2008-3214

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Dnsmasq](#) from [Thekelleys](#) contain the following vulnerability:

dnsmasq 2.25 allows remote attackers to cause a denial of service (daemon crash) by (1) renewing a nonexistent lease or (2) sending a DHCPREQUEST for an IP address that is not in the same network, related to the DHCP NAK response from the daemon.

CVE-2008-3214 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

oss-security - Re: CVE request for dnsmasq DoS

[www.openwall.com](#)
[text/x-python](#)

[MLIST \[oss-security\] 20080708 Re: CVE request for dnsmasq DoS](#)

Dnsmasq – Freecode

[freshmeat.net](#)
[text/html](#)

[CONFIRM freshmeat.net/projects/dnsmasq/?branch_id=1991&release_id=217681](#)

oss-security - CVE request for dnsmasq DoS

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20080630 CVE request for dnsmasq DoS](#)

Bug #47438 "Dnsmasq crashes when renewing non-existent lease" : Bugs : "dnsmasq" package : Ubuntu

[Exploit](#)
[bugs.launchpad.net](#)
[text/html](#)

[CONFIRM bugs.launchpad.net/ubuntu/+source/dnsmasq/+bug/47438](#)

oss-security - Re: CVE request for dnsmasq DoS

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20080703 Re: CVE request for dnsmasq DoS](#)

oss-security - Re: CVE request for dnsmasq

[www.openwall.com](#)

[MLIST \[oss-security\] 20080701 Re: CVE request for](#)

DoS	text/html	dnsmasq DoS
oss-security - Re: CVE request for dnsmasq DoS	www.openwall.com text/html	MLIST [oss-security] 20080702 Re: CVE request for dnsmasq DoS
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF dnsmasq-multiple-dos(43929)
oss-security - Re: CVE request for dnsmasq DoS	Exploit www.openwall.com text/x-python	MLIST [oss-security] 20080712 Re: CVE request for dnsmasq DoS
	www.thekelleys.org.uk text/plain	CONFIRM www.thekelleys.org.uk/dnsmasq/CHANGELOG

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thekelleys	Dnsmasq	2.25	All	All	All
Application	Thekelleys	Dnsmasq	2.25	All	All	All
cpe:2.3:a:thekelleys:dnsmasq:2.25:*:*:*:*:*:						
cpe:2.3:a:thekelleys:dnsmasq:2.25:*:*:*:*:*:						

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)