



CVE-2022-33990

Published on: Not Yet Published

Last Modified on: 08/18/2022 04:54:00 PM UTC

CVE-2022-33990

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Dproxy-nexgen](#) from [Dproxy-nexgen Project](#) contain the following vulnerability:

Misinterpretation of special domain name characters in dproxy-nexgen (aka dproxy nexgen) leads to cache poisoning because domain names and their associated IP addresses are cached in their misinterpreted form.

CVE-2022-33990 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVE References

Description	Tags	Link
dproxy - caching DNS proxy download SourceForge.net	sourceforge.net text/html	MISC sourceforge.net/projects/dproxy/
Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS USENIX	www.usenix.org text/html	MISC www.usenix.org/conference/usenixsecurity21/presentation/jeitner
XDRI Attacks - and - How to Enhance Resilience of Residential Routers USENIX	www.usenix.org text/html	MISC www.usenix.org/conference/usenixsecurity22/presentation/jeitner
oss-security - Multiple DNS Cache poisoning vulnerabilities in dproxy and dproxy-nexgen (CVE-2022-33988, CVE-2022-33989, CVE-2022-33990, CVE-2022-33991)	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2022/08/14/3

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.

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content that are linked, presented on these sites. 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	Dproxy-nexgen Project	Dproxy-nexgen	-	All	All	All
cpe:2.3:a:dproxy-nexgen_project:dproxy-nexgen:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-33990 : Misinterpretation of special domain name characters in dproxy-nexgen aka dproxy nexgen leads to... twitter.com/i/web/status/1...	2022-08-15 13:07:48
 /r/netcve	CVE-2022-33990	2022-08-15 14:38:13

[← Previous ID](#)

[Next ID →](#)

© CVEreport 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](#).

CVEreport and Source URL Uptime Status [status.cve.report](#)