



CVE-2021-23270

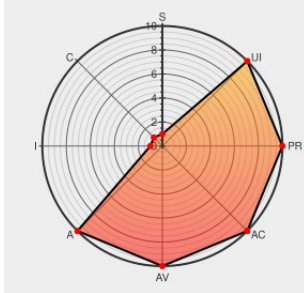
Published on: 04/12/2021 12:00:00 AM UTC

Last Modified on: 04/27/2021 03:04:00 PM UTC

CVE-2021-23270

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

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



Certain versions of [Gargoyle](#) from [Gargoyle-router](#) contain the following vulnerability:

In Gargoyle OS 1.12.0, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set.

CVE-2021-23270 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	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix IPv6 routing loops · ericpaulbishop/gargoyle@24afe94	github.com text/html	MISC github.com/ericpaulbishop/gargoyle/commit/24afe944a6ffff53d84a748384e276a4e95912ec

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	Gargoyle-router	Gargoyle	1.12.0	All	All	All
cpe:2.3:a:gargoyle-router:gargoyle:1.12.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23270 : In Gargoyle OS 1.12.0, when IPv6 is used, a routing loop can occur that generates excessive network... twitter.com/i/web/status/1...	2021-04-12 19:05:26
 @0_exploit	CVE-2021-23270 dlvr.it/RxXC3f	2021-04-12 22:33:03
 /r/netcve	CVE-2021-23270	2021-04-12 19:10:09

[← 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