



CVE-2022-28224

Published on: Not Yet Published

Last Modified on: 06/14/2022 03:32:00 PM UTC

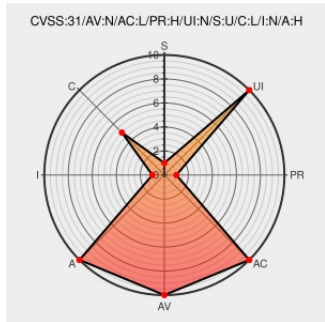
CVE-2022-28224

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Calico Enterprise](#) from [Tigera](#) contain the following vulnerability:

Clusters using Calico (version 3.22.1 and below), Calico Enterprise (version 3.12.0 and below), may be vulnerable to route hijacking with the floating IP feature. Due to insufficient validation, a privileged attacker may be able to set a floating IP annotation to a pod even if the feature is not enabled. This may allow the attacker to intercept and reroute traffic to their compromised pod.

CVE-2022-28224 has been assigned by psirt@tigera.io to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Tigera - Calico Enterprise** version <= v3.12.0

Affected Vendor/Software: **Project Calico - Calico** version <= v3.22.1

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Security Bulletins – TTA-2022-001	www.tigera.io text/html	MISC www.tigera.io/security-bulletins-tta-2022-001/
-----------------------------------	---	--

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	Tigera	Calico Enterprise	All	All	All	All
Application	Tigera	Calico Enterprise	3.12.0	All	All	All
Operating System	Tigera	Calico Os	All	All	All	All

cpe:2.3:a:tigera:calico_enterprise:*:*:*:*:*:*:

cpe:2.3:a:tigera:calico_enterprise:3.12.0:*:*:*:*:*:*:

cpe:2.3:o:tigera:calico_os:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-28224 : Clusters using Calico version 3.22.1 and below , Calico Enterprise version 3.12.0 and below , ma... twitter.com/i/web/status/1...	2022-06-06 18:12:45
@LinInfoSec	Calico - CVE-2022-28224: tigera.io/security-bulle...	2022-06-06 22:00:28
/r/netcve	CVE-2022-28224	2022-06-06 19:38:59

[← 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