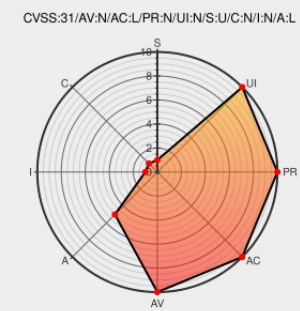
CVE-2022-27889

Published on: Not Yet Published

Last Modified on: 06/23/2022 04:22:00 PM UTC

CVE-2022-27889 - advisory for PLTRSEC-2022-02

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Foundry Multipass from Palantir contain the following vulnerability:

The Multipass service was found to have code paths that could be abused to cause a denial of service for authentication or authorization operations. A malicious attacker could perform an application-level denial of service attack, potentially causing authentication and/or authorization operations to fail for the duration of the attack. This could lead to performance degradation or login failures for customer Palantir Foundry environments. This vulnerability is resolved in Multipass 3.647.0. This issue affects: Palantir Foundry Multipass versions prior to 3.647.0.

CVE-2022-27889 has been assigned by cve-coordination@palantir.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Palantir** - **Foundry Multipass** version **< 3.647.0**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
security-bulletins/PLTRSEC-2022-02.md at main · palantir/security-bulletins · GitHub	github.com text/html	MISC github.com/palantir/security-bulletins/blob/main/PLTRSEC-2022-02.md

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	Palantir	Foundry Multipass	All	All	All	All

cpe:2.3:a:palantir:foundry_multipass:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was identified internally at Palantir. Initial activity was observed as a result of good-faith security research conducted by bug bounty participants.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-27889 : The Multipass service was found to have code paths that could be abused to cause a denial of servi… twitter.com/i/web/status/1…	2022-06-14 13:50:12
/r/netcve	CVE-2022-27889	2022-06-14 14:38:36

← Previous ID

Next ID→