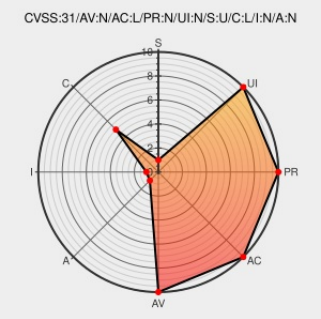
CVE-2022-27891

Published on: Not Yet Published

Last Modified on: 07/18/2023 01:55:00 PM UTC

CVE-2022-27891 - advisory for PLTRSEC-2022-10

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



Certain versions of Gotham from Palantir contain the following vulnerability:

Palantir Gotham included an unauthenticated endpoint that listed all active usernames on the stack with an active session. The affected services have been patched and automatically deployed to all Apollo-managed Gotham instances. It is highly recommended that customers upgrade all affected services to the latest version. This issue affects: Palantir Gotham versions prior to 103.30221005.0.

CVE-2022-27891 has been assigned by cve-coordination@palantir.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Palantir** - **Gotham** version **< 3.22.10.4**

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
security-bulletins/PLTRSEC-2022-10.md at main · palantir/security-bulletins · GitHub	github.com text/html	MISC github.com/palantir/security-bulletins/blob/main/PLTRSEC-2022-10.md

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Palantir Gotham included an unauthenticated endpoint that listed all active usernames on the stack with an active ses…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Palantir	Gotham	All	All	All	All

cpe:2.3:o:palantir:gotham:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-27891 : Palantir Gotham included an unauthenticated endpoint that listed all active usernames on the stack… twitter.com/i/web/status/1…	2023-02-16 16:03:10
@doogsineerg	New vulnerability on the NVD: CVE-2022-27891 ift.tt/9ChW1Jc	2023-02-16 17:33:08
@Tickertick_saas	CVE-2022-27891 - Palantir Gotham included an unauthenticated endpoint that listed ... More… twitter.com/i/web/status/1…	2023-02-16 17:56:56
@RedPacketSec	Palantir Gotham information disclosure | CVE-2022-27891 - redpacketsecurity.com/palantir-gotha… #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-02-20 10:02:18
/r/netcve	CVE-2022-27891	2023-02-16 16:38:13

← Previous ID

Next ID→