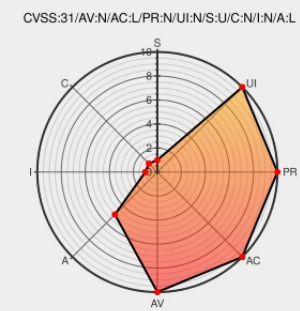
CVE-2022-27897

Published on: Not Yet Published

Last Modified on: 02/24/2023 06:40:00 PM UTC

CVE-2022-27897 - advisory for PLTRSEC-2022-12

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



Certain versions of Gotham from Palantir contain the following vulnerability:

Palantir Gotham versions prior to 3.22.11.2 included an unauthenticated endpoint that would load portions of maliciously crafted zip files to memory. An attacker could repeatedly upload a malicious zip file, which would allow them to exhaust memory resources on the dispatch server.

CVE-2022-27897 has been assigned by cve-coordination@palantir.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Palantir** - **Gotham** version **< 3.22.11.2**

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

CVE References

Description	Tags	Link
security-bulletins/PLTRSEC-2022-12.md at main · palantir/security-bulletins · GitHub	github.com text/html	MISC github.com/palantir/security-bulletins/blob/main/PLTRSEC-2022-12.md

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Palantir Gotham versions prior to 3.22.11.2 included an unauthenticated endpoint that would load portions of maliciou…

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-2022-27897 : Palantir Gotham versions prior to 3.22.11.2 included an unauthenticated endpoint that would load p… twitter.com/i/web/status/1…	2023-02-16 16:03:56
@doogsineerg	New vulnerability on the NVD: CVE-2022-27897 ift.tt/VNaT3CK	2023-02-16 17:33:06
/r/netcve	CVE-2022-27897	2023-02-16 16:38:15

← Previous ID

Next ID→