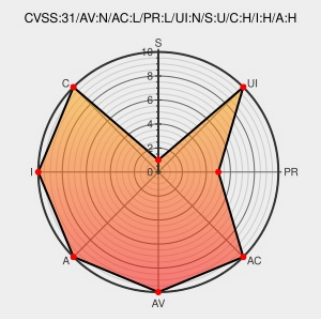
CVE-2023-22951

Published on: Not Yet Published

Last Modified on: 04/24/2023 02:43:00 PM UTC

CVE-2023-22951

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



Certain versions of Cloud from Tigergraph contain the following vulnerability:

An issue was discovered in TigerGraph Enterprise Free Edition 3.x. It creates an authentication token for internal systems use. This token can be read from the configuration file. Using this token on the REST API provides an attacker with anonymous admin-level privileges on all REST API endpoints.

CVE-2023-22951 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Unsecured Web Credentials - Neo4j Graph Data Platform	neo4j.com text/html	MISC neo4j.com/security/cve-2023-22951/
Latest Announcements topics - TigerGraph	dev.tigergraph.com text/html	MISC dev.tigergraph.com/forum/c/tg-community/announcements/35

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tigergraph	Cloud	-	All	All	All
Application	Tigergraph	Tigergraph Enterprise	3.7.0	All	All	All
Application	Tigergraph	Tigergraph Enterprise	3.7.0	All	All	All

cpe:2.3:a:tigergraph:cloud:-:*:*:*:*:*:*:*:

cpe:2.3:a:tigergraph:tigergraph_enterprise:3.7.0:*:*:*:free:-:*:*:

cpe:2.3:a:tigergraph:tigergraph_enterprise:3.7.0:*:*:*:free:docker:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22951 : An issue was discovered in TigerGraph Enterprise Free Edition 3.x. It creates an authentication to… twitter.com/i/web/status/1…	2023-04-13 20:09:32

← Previous ID

Next ID→