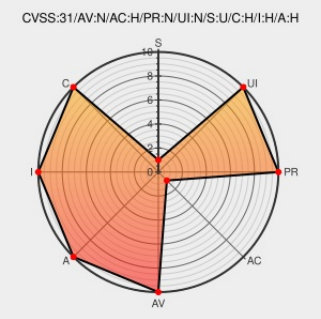
CVE-2022-24827

Published on: Not Yet Published

Last Modified on: 04/19/2022 03:20:00 PM UTC

CVE-2022-24827 - advisory for GHSA-8xpj-9j9g-fc9r

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



Certain versions of Elide from Elide contain the following vulnerability:

Elide is a Java library that lets you stand up a GraphQL/JSON-API web service with minimal effort. When leveraging the following together: Elide Aggregation Data Store for Analytic Queries, Parameterized Columns (A column that requires a client provided parameter), and a parameterized column of type TEXT. There is the potential for a hacker to provide a carefully crafted query that would bypass server side authorization filters through SQL injection. A recent patch to Elide 6.1.2 allowed the '-' character to be included in parameterized TEXT columns. This character can be interpreted as SQL comments ('--') and allow the attacker to remove the WHERE clause from the generated query and bypass authorization filters. A fix is provided in Elide 6.1.4. The vulnerability only exists for parameterized columns of type TEXT and only for analytic queries (CRUD is not impacted). Workarounds include leveraging a different type of parameterized column (TIME, MONEY, etc) or not leveraging parameterized columns.

CVE-2022-24827 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **yahoo** - **elide** version **= 6.1.3**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in elide-datastore-aggregation · Advisory · yahoo/elide · GitHub	github.com text/html	CONFIRM github.com/yahoo/elide/security/advisories/GHSA-8xpj-9j9g-fc9r
Release 6.1.4 · yahoo/elide · GitHub	github.com text/html	MISC github.com/yahoo/elide/releases/tag/6.1.4
Revert "Update: Make `-` a valid TEXT value type character" by aklish · Pull Request #2581 · yahoo/elide · GitHub	github.com text/html	MISC github.com/yahoo/elide/pull/2581

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elide	Elide	6.1.3	All	All	All

cpe:2.3:a:elide:elide:6.1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	cve.report/CVE-2022-24827 Elide is a Java library that lets you stand up a GraphQL/JSON-API web service with minimal… twitter.com/i/web/status/1…	2022-04-11 22:16:38
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-24827 Elide is a Java library that lets you stand up a GraphQL/JSON-API… twitter.com/i/web/status/1…	2022-04-11 23:56:00
/r/netcve	CVE-2022-24827	2022-04-11 23:40:51

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report