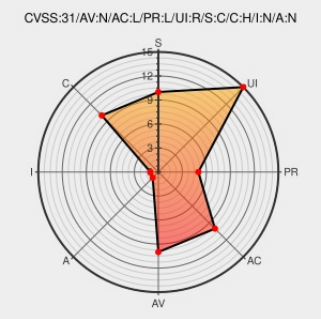
CVE-2020-5289

Published on: 03/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5289 - advisory for GHSA-2mxr-89gf-rc4v

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



Certain versions of Elide from Elide contain the following vulnerability:

In Elide before 4.5.14, it is possible for an adversary to "guess and check" the value of a model field they do not have access to assuming they can read at least one other field in the model. The adversary can construct filter expressions for an inaccessible field to filter a collection. The presence or absence of models in the returned collection can be used to reconstruct the value of the inaccessible field. Resolved in Elide 4.5.14 and greater.

CVE-2020-5289 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **yahoo** - **elide** version **< 4.5.14**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
Enforce ReadPermission for filter joins by wcekan · Pull Request #1236 · yahoo/elide · GitHub	Patch github.com text/html	MISC github.com/yahoo/elide/pull/1236/commits/a985f0f9c448aabe70bc904337096399de4576dc
Enforce ReadPermission for filter joins by wcekan · Pull Request #1236 · yahoo/elide · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/yahoo/elide/pull/1236
Read permissions not enforced for client provided filter expressions. · Advisory · yahoo/elide · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/yahoo/elide/security/advisories/GHSA-2mxr-89gf-rc4v

Related QID Numbers

983120 Java (maven) Security Update for com.yahoo.elide:elide-core (GHSA-2mxr-89gf-rc4v)

Known Affected Configurations (CPE V2.3)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→