Multiple Reflected XSS Vulnerabilities in error handlers in zadam/trilium

0

Valid Reported on Jun 28th 2022

Description

Multiple routing error handlers are vulnerable to reflected XSS.

Proof of Concept

Deploy `trilium` server and access to these endpoint will execute the alert js function.

```
http://localhost:8080/custom/%3Cscript%3Ealert(1)%3C/script%3E
http://localhost:8080/share/api/notes/%3Cimg%20src=x%20onerror=alert(1)%3E
http://localhost:8080/share/api/notes/%3Cimg%20src=x%20onerror=alert(1)%3E/
http://localhost:8080/share/api/images/%3Cimg%20src=x%20onerror=alert(1)%3E
http://localhost:8080/share/api/notes/%3Cimg%20src=x%20onerror=alert(1)%3E/
```

Impact

According to OWASP:
XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirect the user to some other page or site, or modify presentation of content. An XSS vulnerability allowing an attacker to modify a press release or news item could affect a company's stock price or lessen consumer confidence. An XSS vulnerability on a pharmaceutical site could allow an attacker to modify dosage information resulting in an overdose.

Occurrences

JS routes.js L86

```
/share/api/notes/:noteId
```

JS routes.js L125

```
/share/api/images/:noteId/:filename
```

JS routes.js L101

```
/share/api/notes/:noteId/download
```

CVE
CVE-2022-2290
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.4)

Registry
Other

Affected Version
<=0.52.3

Visibility
Public

Status
Fixed

Found by

Khang Vo (doublevkay)
@vovikhangcdv
master

This report was seen 684 times.

We are processing your report and will contact the **zadam/trilium** team within 24 hours.
5 months ago

Khang Vo (doublevkay) modified the report 5 months ago

We have contacted a member of the **zadam/trilium** team and are waiting to hear back
5 months ago

We have sent a follow up to the **zadam/trilium** team. We will try again in 7 days. 5 months ago

zadam 5 months ago Maintainer

Hi, thanks for reporting this. This has been fixed in 0.52.4 and 0.53.1-beta by using correct content-type (text/plain).

Fortunately, this is quite difficult to exploit given that Trilium is deployed on the user's server, attacker needs the URL address of the user's server and their contact (to send personalized malicious link).

zadam modified the Severity from High (7.3) to Medium (6.4) 5 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

zadam validated this vulnerability 5 months ago

Khang Vo (doublevkay) has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

zadam marked this as fixed in **0.52.4, 0.53.1-beta** with commit **3faae6** 5 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

routes.js#L125 has been validated ✔

routes.js#L101 has been validated ✔

routes.js#L86 has been validated ✔

Sign in to join this conversation