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

0

Valid Reported on Nov 18th 2021

Description

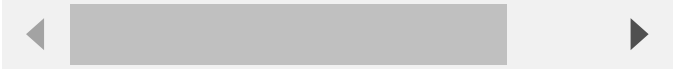
Cross site scripting vulnerability in name field on customer edit form

Proof of Concept

```
place this payload in customer name field    and save  "><iMg SrC="x" oNeRR

# Impact

This vulnerability is capable of stolen the user session
```



References

- https://portswigger.net/web-security/cross-site-scripting

CVE
CVE-2021-3983
(Published)

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

Severity
Medium (6.3)

Visibility
Public

Status
Fixed

Found by

Asura-N
@asura-n
noisy

Fixed by

Kevin Papst
@kevinpapst
unranked

This report was seen 362 times.

We are processing your report and will contact the **kevinpapst/kimai2** team within 24 hours. a year ago

We have contacted a member of the **kevinpapst/kimai2** team and are waiting to hear back a year ago

Kevin Papst validated this vulnerability a year ago

Asura-N has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Kevin Papst a year ago Maintainer

I worked on that before and thought it was fixed, but seems the Javascript was still broken. Thanks for the report @Asura-N !

Kevin Papst submitted a patch a year ago

Kevin Papst marked this as fixed in 1.16.3 with commit 89bfa8 a year ago

Kevin Papst has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

Jamie Slome a year ago

Admin

CVE published! 🎊

Sign in to join this conversation