Stored XSS in "Name", "Group Name" & "Title" in polonel/trudesk

0

Valid Reported on Mar 23rd 2022

Description

The application allows img tag & src attribute in "Name","Title" & "Group Name" fields for which attackers can perform stored cross-site scripting.

Proof of Concept

1.Login to the application and go to profile.
2.Now in the "Name" input field paste the below payload and click on "SAVE"
<img src=1 onerror=prompt(document.domain)>
3.After that when you go to any other page then XSS will trigger.

Please check the below sub-reports for other Vulnerable input fields:-

https://huntr.dev/bounties/6fc958d2-ec3b-4319-ac4a-eccec03908bb/
https://huntr.dev/bounties/b9c50ca6-99d5-48d4-ba2c-f5c50179aa3a/

Video PoC

https://drive.google.com/file/d/1dL1OXVye1tFEQuTqJpdE_aSCPcE9uj0S/view?usp=sharing
https://drive.google.com/file/d/1hK8W0u1Jjz424O44X_nEVrrU_CVReTT9/view?usp=sharing
https://drive.google.com/file/d/15kuPCDYI9nrFm1WXB0FFBQzkLU5Xtrly/view?usp=sharing

Impact

This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.

CVE

CVE-2022-1290
(Published)

Vulnerability Type

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

Severity
Critical (9)

Registry
Other

Affected Version
v1.1.11 - v1.0.6

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

This report was seen 649 times.

We are processing your report and will contact the **polonel/trudesk** team within 24 hours. 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

We have contacted a member of the **polonel/trudesk** team and are waiting to hear back 8 months ago

We have sent a follow up to the **polonel/trudesk** team. We will try again in 7 days. 8 months ago

SAMPRIT DAS 8 months ago

@admin any update?

Jamie Slome 8 months ago Admin

Please allow for our automated notification system to contact the maintainer. Once the report has gone stale, feel free to get in touch again and we will personally reach out to the maintainers.

A **polonel/trudesk** maintainer has acknowledged this report 8 months ago

Chris Brame 8 months ago Maintainer

Please modify the report to include the following sub-reports you created.

https://huntr.dev/bounties/6fc958d2-ec3b-4319-ac4a-eccec03908bb/
https://huntr.dev/bounties/b9c50ca6-99d5-48d4-ba2c-f5c50179aa3a/

These reports are the same and should cover that XSS is allowed in input fields. A separate report for each input field is unwarranted.

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS 8 months ago Researcher

@maintainer Done I have modified the report now can you please validate it.

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS 8 months ago

@maintainer also please give permission to admin to register a CVE for this report

Chris Brame validated this vulnerability 8 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

SAMPRIT DAS 8 months ago Researcher

@admin Can you assign a CVE for this report?

Jamie Slome 8 months ago Admin

We can assign a CVE if the maintainer is happy for one to be assigned and published.

@maintainer - thoughts?

We have sent a fix follow up to the **polonel/trudesk** team. We will try again in 7 days.
8 months ago

SAMPRIT DAS 8 months ago Researcher

@maintainer @polonel Can you please reply?

Chris Brame 8 months ago Maintainer

@researcher Thank you for your report. No fix has been made yet and this report will get updated when a fix is pushed to master. Please be patient. I am a solo dev working on Trudesk as a hobby. Sometimes it takes weeks for these things to get resolved. Bombarding me with emails and report update requests will not speed this process up. As always with OSS, pull requests are always welcome. Thanks.

SAMPRIT DAS 8 months ago Researcher

@maintainer @polonel I am not asking about a fix actually I am asking that can you please give permission to admin to assign a CVE number to this report.

Chat with us

Jamie Slome 8 months ago Admin

@sampritdas8 - please stop spamming the comments section. Once the maintainer has confirmed a fix, we can see about assigning and publishing a CVE. Please be patient.

If further spamming continues in the comments section, action will be taken against your account.

Chris Brame marked this as fixed in **v1.2.0** with commit **4f48b3** 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Chris Brame 8 months ago — Maintainer

Fix has been pushed to master and released in version 1.2.0
CVE can be assigned and published.

SAMPRIT DAS 8 months ago — Researcher

@admin Maintainer has given permission now can you please register CVE for this report?

Jamie Slome 8 months ago — Admin

Sorted 👍

Sign in to join this conversation

.