huntr

Reflected XSS on ticket filter function in polonel/trudesk

0



Reported on May 5th 2022

Description

Ticket management filter in Trudesk v1.2.0 allow user to perform XSS due to improper validation on filter attribute such as "status", "ticket type", "assignee" and etc.

Proof of Concept

Login to Trudesk with role user privilege
Tickets -> Filter ticket
Filter for ticket status (poc on attribute status)
Insert payload in the filter result

Endpoint

http://{IP}/tickets/filter/

Payload used

">

Screenshot POC

ticket filter xss domain xss cookie

Impact

This vulnerability is capable of executing a malicious javascript code in web page

Occurrences

Chat with us

CVE

CVE-2022-1719 (Published)

Vulnerability Type

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

Severity

Medium (5.5)

Registry

Other

Affected Version

v120

Visibility

Public

Status

Fixed

Found by

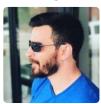


din

@baharuddinzulkifli



Fixed by



Chris Brame

apolone

unranked 🗸

This report was seen 564 times.

We are processing your report and will contact the **polonel/trudesk** team within 24 hours. 7 months ago

din modified the report 7 months ago

Chat with us

din modified the report 7 months ago din modified the report 7 months ago din modified the report 7 months ago We have contacted a member of the polonel/trudesk team and are waiting to hear back We have sent a follow up to the polonel/trudesk team. We will try again in 7 days. 7 months ago din 6 months ago Researcher hi team, any update from this report A polonel/trudesk maintainer has acknowledged this report 6 months ago Chris Brame assigned a CVE to this report 6 months ago Chris Brame validated this vulnerability 6 months ago din has been awarded the disclosure bounty ✓ The fix bounty is now up for grabs The researcher's credibility has increased: +7 Chris Brame marked this as fixed in 1.2.2 with commit 36a542 6 months ago Chris Brame has been awarded the fix bounty 🗸 This vulnerability will not receive a CVE x tickets.js#L217-L261 has been validated 🗸 din 6 months ago Researcher Thanks for validating this Chat with us

Sign in to join this conversation

2022 © 418sec

L	 	4.	
\mathbf{r}	 \mathbf{n}	т	r

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team