huntr

Stored XSS viva .svg file upload in polonel/trudesk

0

✓ Valid Reported on Mar 19th 2022

Description

The application allows .svg files to upload which lead to stored XSS

Proof of Concept

1.Download the payload from this link:-
https://drive.google.com/file/d/1c1BP5bxXBxtwLfRJTrEPgMWK1yVFDF2R/view?usp=sharing
and upload it on your profile.
2.Now open the path of the uploaded image (Either by right click on image then copy image address OR right-click, inspect the image, the URL will come in the inspect, edit it as HTML)
3.Then XSS will trigger for allowing malicious svg extension.

Video PoC

https://drive.google.com/file/d/1_KOXMP_-jMhF4jEtg6XI_NopDNp5ZRCM/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-2022-1045
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9)

Visibility
Public

Status

Fixed

Found by

SAMPRIT DAS

@sampritdas8

pro

This report was seen 539 times.

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

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 register a CVE for this?

SAMPRIT DAS 8 months ago Researcher

@admin

Jamie Slome 8 months ago Admin

Sure, @maintainer, can you please confirm whether you would like us to assign and publish a CVE for this report?

SAMPRIT DAS 8 months ago Researcher

@Chris @polonel @maintainer can you please reply

Chat with us

Chris Brame 8 months ago Maintainer

Yes, you can assign and publish a CVE for this report.

SAMPRIT DAS 8 months ago Researcher

@admin Maintainer is agree so can you please register a CVE for this report?

Jamie Slome 8 months ago Admin

CVE assigned! 🎊

Please confirm the fix @maintainer, and then we will be able to publish the CVE.

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

We have sent a second fix follow up to the **polonel/trudesk** team. We will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **polonel/trudesk** team. This report is now considered stale. 8 months ago

Chris Brame marked this as fixed in **v1.2.0** with commit **c4b262** 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

SAMPRIT DAS 8 months ago Researcher

@Chris @polonel @maintainer I am still able to reproduce the step for this report in the 1.2.0 version can you please also verify it from your side?

SAMPRIT DAS 8 months ago Researcher

you can reproduce the step by downloading this SVG payload from this drive link: https://drive.google.com/file/d/1c1BP5bxXBxtwLfRJTrEPgMWK1yVFDF2R/view?usp=sharing

and upload it in the profile Image.

Chat with us

SAMPRIT DAS 8 months ago Researcher

@admin Can you update the CVE details on NVD?

Jamie Slome 8 months ago Admin

Sorted 👍

Sign in to join this conversation