

Cross-site Scripting (XSS) - Stored in combodo/itop

0



Valid

Reported on Jun 30th 2021



BUG

stored xss via file upload



STEP TO REPRODUCE

here in this case i uploaded a html file with xss payload inside.

Plz check this 1 minute video to reproduce

<https://drive.google.com/file/d/1xKqYFgrsFUfp9Ufe4XiATQcAL-Q6Mr9G/view?usp=sharing>



Impact

I see there is many different type of role base user . So, user who has permission to upload document can make xss attack against higher level user or admin

Vulnerability Type

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

Severity

High (8.1)

Affected Version

*

Visibility

Public

Status

Fixed

Found by



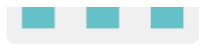
ranjit-git

@ranjit-git

amateur



Chat with us



This report was seen 329 times.

ranjit-git modified the report [a year ago](#)

Z-Old [a year ago](#)

[Admin](#)

Hey ranjit-git, I've just emailed the maintainer and am waiting to hear back. Good job!

We have contacted a member of the **combodo/itop** team and are waiting to hear back
[a year ago](#)

A **combodo/itop** maintainer validated this vulnerability [a year ago](#)

ranjit-git has been awarded the disclosure bounty 

The fix bounty is now up for grabs

A **combodo/itop** maintainer [a year ago](#)

[Maintainer](#)

The fix will be part of 2.7.6 that has just been released.

A GitHub advisory was created : <https://github.com/Combodo/iTop/security/advisories/GHSA-67x5-mqg4-rvgc>

We will publish this page and the advisory in 3 months.

Pierre Goiffon marked this as fixed in **2.7.6** with commit **92a9a8** [8 months ago](#)

The fix bounty has been dropped 

This vulnerability will not receive a CVE 

Pierre Goiffon [8 months ago](#)

[Maintainer](#)

Hi,

Combodo usually send goodies for its contributors, as a way to thank them.

@ranjit-git can you send your postal address to pierre.goiffon @ combodo spaces around the @)?

[Chat with us](#)

@mainatiner

Thanks for such care.

Happy to secure itop project.

I will send postal address to above mail id

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us