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

Valid Reported on Jun 30th 2021

BUG

stored xss via contact lastname

STEP TO REPRODUCE

Plz check this 1 minute video to reproduce
https://drive.google.com/file/d/1bR9ili6jKxX3UQ2dQUQTqNL0e4LsMDtk/view?usp=sharing

Impact

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

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

Pierre Goiffon 7 months ago

Hello,
The vulnerability was fixed in 3.0.0-beta3

Chat with us

The vulnerability was fixed in 3.0.0-beta3
It was only affecting 3.0.0-beta and 3.0.0-beta2

Combodo internal ref is N°4127

We just published a GitHub security advisory : Fix XSS vulnerability in object attribute's tooltip · Advisory · Combodo/iTop

Pierre Goiffon marked this as fixed in **3.0.0-beta3** with commit **ebbf6e** 7 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Sign in to join this conversation

2022 © 418sec

Chat with us