New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Knowledgebase" feature in OsTicket #5514

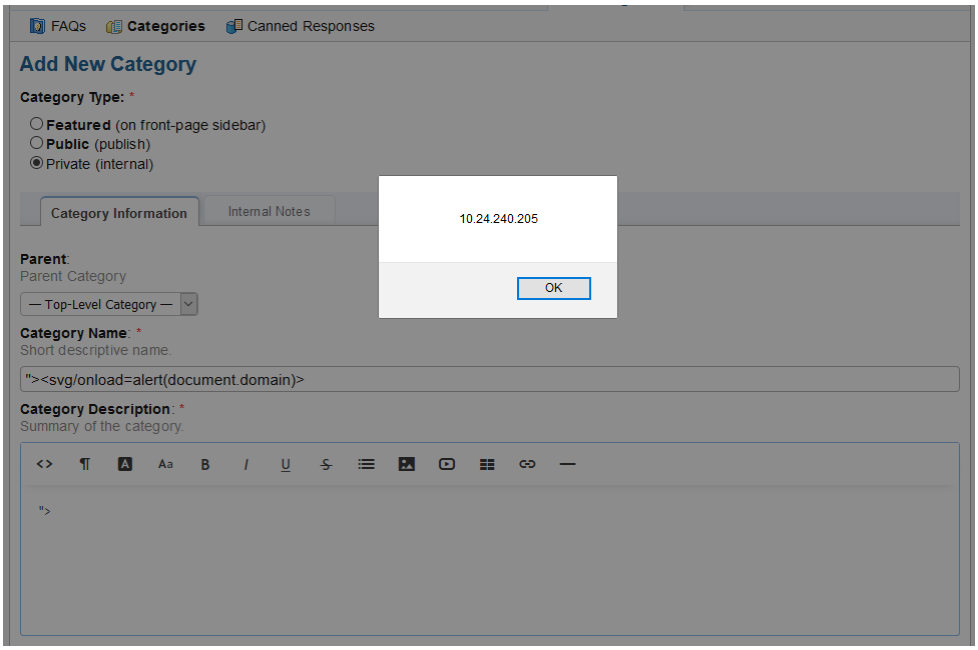
Open **tranvannam186** opened this issue on May 21, 2020 · 3 comments

tranvannam186 commented on May 21, 2020 • edited by JediKev

Description:
A authenticated malicious user can take advantage of a Reflected XSS vulnerability in the "Knowledgebase" feature. This was can be bypassed by using HTML event handlers, such as "ontoggle".
OS: firefox
Steps to Reproduce:

1. Log into the panel OsTicket
2. Go to "/osticket/scp/kb.php"
3. Go to "/osticket/scp/categories.php"
4. Click "Add New Category"
5. Insert payload to Category Name or Category Description:
   `"><svg/onload=alert(document.domain)>`

Expected behavior: [What you expected to happen]
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.
Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.
Screenshots



JediKev commented on May 21, 2020 • edited — Contributor

@tranvannam186

Please refrain from reporting vulnerabilities like this in the future. Please, next time follow Responsible Disclosure practices by reporting directly to us. You can send all POCs to `security[at]osticket[dot]com` . This will give us time to mitigate the vulnerability before it is made public. Luckily this is Low severity as you have to be authenticated as an Agent first.

With this being said, this particular vulnerability has two parts:
1.) Pasting Payload In Editor

- This is an issue with the 3rd party text editor we use called Redactor as the payload executes immediately when pasting into the editor. You will need to report this to the developers of the text editor Imperavi.

2.) Pasting Payload in HTML View and Saving Changes (just so the payload doesn't execute immediately)

- This is an issue where we are not sanitizing the return values on errors. The content is sanitized before saving to the database but if the Category has any errors the content is not sanitized. I will create a patch for this shortly and update this thread.

Cheers.

JediKev mentioned this issue on May 21, 2020

xss: FAQ Category On Errors #5517

Merged

JediKev commented on May 21, 2020 — Contributor

@tranvannam186

Here is the patch to mitigate the 2nd half of the vulnerability:

- xss: FAQ Category On Errors #5517

Please apply the changes, retest, and get back to me.

Cheers.

JediKev commented on Jun 16, 2020 — Contributor

@tranvannam186

Here is a patch that upgrades Redactor to the latest version which mitigates the 1st half of the XSS vulnerability you reported:

- redactor: Upgrade to version 3.4.0 #5553

Cheers.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants