



## Remote Code Execution via the page title using Velocity

## Details

Type:	Bug	Resolution:	Fixed
Priority:	Major	Fix Version/s:	<a href="#">18.0.0-rc-1</a> , <a href="#">17.10.1</a> , <a href="#">17.4.8</a>
Affects Version/s:	17.0.0-rc-1		
Component/s:	<a href="#">Old Core</a>		
Labels:	<a href="#">attack_escalation</a> <a href="#">attacker_script</a> <a href="#">security</a>		
Tests:	Unit		
Difficulty:	Easy		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Similar issues:			

## Description

A Remote Code Execution (RCE) vulnerability exists due to improper handling of user-supplied input within the page title parameter when creating a page by an authenticated user with script permissions, which is processed by the Apache Velocity template engine.

The application dynamically injects the page title value into a Velocity template . As a result, an attacker can inject arbitrary Velocity expressions or malicious template syntax that will be evaluated on the server side and bypass the sandbox of velocity

By crafting a specially designed payload , the attacker can execute arbitrary commands on the underlying operating system with the privileges of the web application. This can lead to full compromise of the affected server, data exfiltration, or lateral movement within the network.

Payloads :

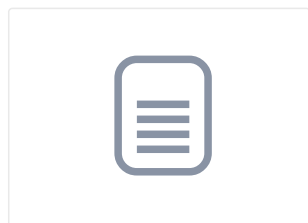
For any user with script permission :

```
$request.request.getServletContext().getAttribute("org.apache.tomcat.InstanceManager").newInstance("org.apache.batik.script.jpythc
os; os.system('touch /tmp/RCE')
```

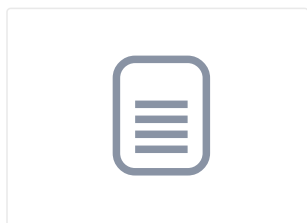
For Admin :

```
$request.getServletContext().getAttribute("org.apache.tomcat.InstanceManager").newInstance("org.apache.batik.script.jpython.JPyth
os; os.system('touch /tmp/RCE')
```

## Attachments



[Exploit\\_user\\_with\\_script\\_pe](#)  
08/Nov/25 20:20 6.86 MB



[Exploit.webm](#)  
07/Nov/25 14:37 6.96 MB



[Function\\_that\\_evaluate\\_the](#)  
07/Nov/25 14:37 915 kB

## Issue Links

## is caused by

[XCOMMONS-2963](#) Upgrade to Servlet 5.0

CLOSED

## is duplicated by

[XWIKI-23702](#) Remote Code Execution via Velocity scripts (Macro)

CLOSED

## links to

 Security Advisory

## Activity

Newest first ▾

- Michael Hamann added a comment - 2 days ago

Thank you [isfake](#), I've just published the advisory and the two Jira issues.

- Youssef Azefzaf added a comment - 2 days ago - edited

[MichaelHamann](#) As agreed last time, I shared the article about the vulnerability. Here's the link : <https://youssefazefzaf.com/posts/cve> — it was a pleasure working with you.

- Michael Hamann added a comment - 19/Mar/26 09:18

[isfake](#) Okay, I've requested a CVE. As you might have seen, GitHub has assigned CVE-2026-33229 to the advisory. Thank you very much for adjusting to our schedule!

- Youssef Azefzaf added a comment - 18/Mar/26 12:41

[MichaelHamann](#) Thank you for getting back to me! I'd like to request the CVE ID now so I can finalize my article and share it on April 8. I had originally planned to publish on March 25, but this works fine as well.

- Michael Hamann added a comment - 18/Mar/26 09:46

[isfake](#) Sorry, I somehow missed your comment four days ago. I've just checked, and the disclosure of the security advisory is scheduled for April 8. Usually, we request the CVE ID only then but we could also request it now (without publishing it) if you need it before April 8.

- Youssef Azefzaf added a comment - 17/Mar/26 14:12

[MichaelHamann](#) any updates ?

- Youssef Azefzaf added a comment - 13/Mar/26 17:49

[MichaelHamann](#)

I hope you're doing well.

I'm following up on this ticket to ask if a CVE ID has been assigned for this vulnerability yet. I'd like to include the CVE number in my research, so if one has been reserved or assigned, could you please share it with me?

If there's any update or timeline regarding the CVE assignment, I'd appreciate knowing.

- Youssef Azefzaf added a comment - 10/Dec/25 14:41

[MichaelHamann](#) Yes, I'd like to have early access to the security advisory and be credited for discovering this vulnerability.

For the attribution, here is my GitHub: <https://github.com/azefzafyoussef>

Thank you for offering credit — I really appreciate it.

- Michael Hamann added a comment - 10/Dec/25 14:22

[isfake](#) I've fixed the vulnerability by requiring programming right for the `getRequest` method (that is triggered by `\$request.request`). I've also created a draft security advisory. If you're registered on GitHub, I can also grant you early access to the advisory and add a direct credit. If you would like to have any specific attribution included in the advisory, let me know.

- Youssef Azefzaf added a comment - 24/Nov/25 16:46



Thanks for the update. I'm okay with waiting until the end of March 2026. And noted — I'll mention in the publication that the behavior is unexpected for script rights. Appreciate you letting me know.

Load 10 older comments

▼ **People**

---

Assignee:

 Michael Hamann 

Reporter:

 Youssef Azefzaf 

Votes:

 0 Vote for this issue

Watchers:

 2 Start watching this issue

▼ **Dates**

---

Created:

07/Nov/25 14:38

Updated:

2 days ago 15:34

Resolved:

10/Dec/25 14:19

Date of First Response:

11/Nov/25 9:04 AM