XWiki Platform / XWIKI-23702

Remote Code Execution via Velocity scripts (Macro)

Details

Type:	Bug	Resolution:	Duplicate
Priority:	Major	Fix Version/s:	None
Affects Version/s:	17.4.7		
Component/s:	Rendering - Velocity Macro, Velocity		
Labels:	attack_escalation, attacker_script, security		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Similar issues:			

Description

A Remote Code Execution (RCE) vulnerability exists in the Velocity macro and can be exploited by an authenticated user with script permissions.
The application allows users to create Velocity scripts; consequently, an attacker can inject arbitrary Velocity expressions or other malicious template syntax that are evaluated server-side, bypassing the Velocity sandbox.
By crafting a specially designed payload, the attacker can execute arbitrary commands on the underlying operating system with the privileges of the web application.

Payload :

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

Attachments

Exploit_Velocity_Macro.wel
08/Nov/25 20:44 9.50 MB

Issue Links

duplicates

XWIKI-23698 Remote Code Execution via the page title using Velocity CLOSED

Activity

People

Assignee:
Simon Urli

Reporter:
Youssef Azefzaf

Votes:

0 Vote for this issue

Watchers:

1 Start watching this issue

Dates

Created:

08/Nov/25 20:45

Updated:

2 days ago 15:32

Resolved:

12/Nov/25 10:41