



[← To plugin page](#)

 Verified  Not fixed

## WordPress Team Manager plugin <= 1.6.9 - Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities



CVSS 3.1 score  
Medium severity



 Monitoring

Not reported to be exploited

Report



Find out about vulnerable plugins in your websites for free.



Scan your website >

Type	 Plugin	
Vulnerable versions	<= 1.6.9	
Fixed in	N/A	
PSID 	30c572817613	
CVE ID 	 CVE-2022-29406	
Classification 	Cross Site Scripting (XSS)	
OWASP Top 10 	A7: Cross-Site Scripting (XSS)	
Required privilege 	Requires contributor or higher role user authentication.	
Credits	 Ngo Van Thien (Alliance project)	
Publicly disclosed	2022-06-14	

## Details

Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities were discovered by Ngo Van Thien (Patchstack Alliance) in the WordPress Team Manager plugin (versions <= 1.6.9).

## Solution

**Deactivate and delete.** No reply from the vendor.

## References

No other known vulnerabilities found for WordPress Team Manager.  
Let us know if we missed something.

+ Report a vulnerability

**Submit vulnerabilities and become  
a verified Alliance member**

Learn more >

**\$1500**

MONTHLY POOL



[WordPress security](#)

[Patchstack for WordPress](#)

[Plugin auditing](#)

[For agencies](#) **NEW**

[Vulnerability database](#)

[Pricing & features](#)

[Vulnerability API](#)

[Documentation](#)

[Bug bounty program](#) **BETA**

[Changelog](#)

[About us](#)

[Careers](#)

[Media kit](#)

[Insights & articles](#)



[DPA](#)

[Privacy Policy](#)

[Terms & Conditions](#)