

WordPress uListing Plugin <= 2.0.5 is vulnerable to Privilege Escalation

9.8

Critical severity
CVSS 3.1 score

Not known to be exploited

[Report an attack](#)

Protect your sites with automated security

[Enable Protection >](#)

Solution Fixed

Update the WordPress uListing plugin to the latest available version (at least 2.0.6).

Details Show technical details

Vlad Vector discovered and reported this Privilege Escalation vulnerability in WordPress uListing Plugin. This could allow a malicious actor to escalate their low privileged account to something with higher privileges. After this they could take full control of the website. This vulnerability has been fixed in version 2.0.6.

11 other known vulnerabilities for this plugin

[To plugin page >](#)

Authenticated Insecure Direct Object References (IDOR) vulnerability <= 2.0.5

7.1 27.07.2021

Authenticated Reflected CrossSite Scripting (XSS) vulnerability <= 2.0.5

4.8 27.07.2021

Multiple CrossSite Request Forgery (CSRF) vulnerabilities <= 2.0.5

5.4 27.07.2021

Modify User Roles via CrossSite Request Forgery (CSRF) vulnerability <= 2.0.5

6.5 27.07.2021

Settings Update via CrossSite Request Forgery (CSRF) vulnerability <= 2.0.5

4.3 27.07.2021

Report to Patchstack Alliance bounty platform and earn monthly cash prizes.

[Learn more >](#)



Plugin auditing

Vulnerability database

Vulnerability API

Bug bounty program

Patchstack

About us

Careers 

Media Kit

Articles & insights

Whitepaper 2021

For agencies **NEW**

For hosts

Pricing & features

Documentation

Social

 LinkedIn

 Facebook

 Twitter

 hackuu

 Join Discord



[DPA](#) [Privacy Policy](#) [Terms & Conditions](#) © 2022

