



CVE-2021-36920

Published on: 01/14/2022 12:00:00 AM UTC

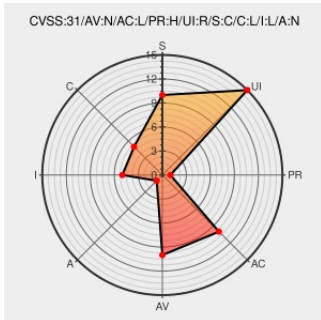
Last Modified on: 01/14/2022 09:37:00 PM UTC

CVE-2021-36920

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Download Monitor WordPress Plugin](#) from [WPChill](#) contain the following vulnerability:

Authenticated Reflected Cross-Site Scripting (XSS) vulnerability discovered in WordPress plugin Download Monitor (versions <= 4.4.6).

CVE-2021-36920 has been assigned by audit@patchstack.com to track the vulnerability

Affected Vendor/Software: **WPChill - Download Monitor (WordPress plugin) version <= 4.4.6**

CVE References

Description	Tags	Link
WordPress Download Monitor plugin <= 4.4.6 - Authenticated Reflected Cross-Site Scripting (XSS) vulnerability - Patchstack	patchstack.com text/html	<input type="checkbox"/> CONFIRM patchstack.com/database/vulnerability/download-monitor/wordpress-download-monitor-plugin-4-4-6-authenticated-reflected-cross-site-scripting-xss-vulnerability
Download Monitor – WordPress plugin WordPress.org	wordpress.org text/html	<input checked="" type="checkbox"/> CONFIRM wordpress.org/plugins/download-monitor/#developers

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE


Known Affected Software

Vendor	Product	Version
WPChill	Download_Monitor_WordPress_plugin	<= 4.4.6

Discovery Credit

Vulnerability discovered by Nguy Minh Tuan (Patchstack Red Team project)

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2021-36920 : Authenticated Reflected Cross-Site Scripting #XSS vulnerability discovered in WordPress plugin D... twitter.com/i/web/status/1...	2022-01-14 20:12:51

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)