

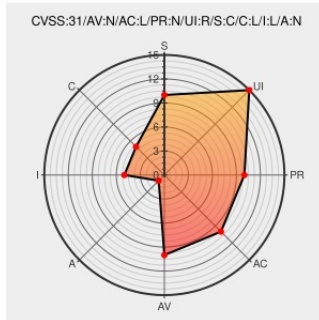


CVE-2021-39320

Published on: 09/01/2021 12:00:00 AM UTC

Last Modified on: 09/08/2021 06:52:00 PM UTC

CVE-2021-39320

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Underconstruction](#) from [Underconstruction Project](#) contain the following vulnerability:

The underConstruction plugin <= 1.18 for WordPress echoes out the raw value of ``$GLOBALS['PHP_SELF']`` in the ucOptions.php file. On certain configurations including Apache+modPHP, this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.

CVE-2021-39320 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Noah Kagan - **underConstruction** version <= 1.18

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Vulnerability Advisories -	www.wordfence.com	MISC www.wordfence.com/vulnerability-advisories/#CVE-2021-39320

Wordfence

text/html

Attention Required! | Cloudflare

wpscan.com

text/html

Inactive Link

Not Archived

MISC

wpscan.com/vulnerability/49ae1df0-d6d2-4cbb-9a9d-bf3599429875

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 Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Underconstruction Project	Underconstruction	All	All	All	All
cpe:2.3:a:underconstruction_project:underconstruction:*:*:*:*:wordpress:*:*						

Discovery Credit

Ramuel Gall, Wordfence

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39320 : The underConstruction plugin <= 1.18 for WordPress echoes out the raw value of `GLOBALS['PHP_SELF... twitter.com/i/web/status/1...	2021-09-01 15:25:05
@LinInfoSec	Wordpress - CVE-2021-39320: wpscan.com/vulnerability/...	2021-09-01 16:50:58

← Previous ID

Next ID →