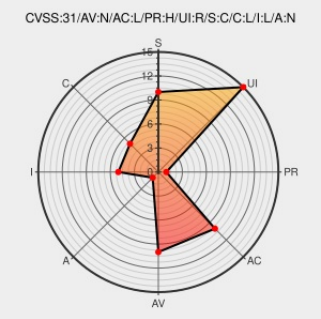
CVE-2022-29418

Published on: Not Yet Published

Last Modified on: 05/05/2022 06:30:00 PM UTC

CVE-2022-29418

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Night Mode from Night Mode Project contain the following vulnerability:

Authenticated (admin user role) Persistent Cross-Site Scripting (XSS) in Mark Daniels Night Mode plugin <= 1.0.0 on WordPress via vulnerable parameters: &ntmode_page_setting[enable-me], &ntmode_page_setting[bg-color], &ntmode_page_setting[txt-color], &ntmode_page_setting[anc_color].

CVE-2022-29418 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mark Daniels** - **Night Mode (WordPress plugin)** version **<= 1.0.0**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Night Mode by WordPress – WordPress plugin |	wordpress.org	CONFIRM wordpress.org/plugins/night-mode/#developers

WordPress.org	text/html	
WordPress Night Mode plugin <= 1.0.0 - Authenticated Persistent Cross-Site Scripting (XSS) vulnerability - Patchstack	patchstack.com text/html	CONFIRM patchstack.com/database/vulnerability/night-mode/wordpress-night-mode-plugin-1-0-0-authenticated-persistent-cross-site-scripting-xss-vulnerability

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	Night Mode Project	Night Mode	All	All	All	All

cpe:2.3:a:night_mode_project:night_mode:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Vulnerability discovered by Ex.Mi (Patchstack)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29418 : Authenticated admin user role Persistent Cross-Site Scripting #XSS in Mark Daniels Night Mode… twitter.com/i/web/status/1…	2022-04-25 17:07:25
/r/netcve	CVE-2022-29418	2022-04-25 18:42:03

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report