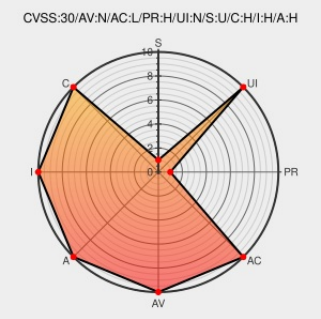
CVE-2019-9572

Published on: 03/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9572

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



Certain versions of Schoolcms from Schoolcms contain the following vulnerability:

SchoolCMS version 2.3.1 allows file upload via the theme upload feature at admin.php?m=admin&c=theme&a=upload by using the .zip extension along with the _Static substring, changing the Content-Type to application/zip, and placing PHP code after the ZIP header. This ultimately allows execution of arbitrary PHP code in Public\Home\1_Static.php because of mishandling in the Application\Admin\Controller\ThemeController.class.php Upload() function.

CVE-2019-9572 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SchoolCMS File Upload Vuln - Issue #2	Exploit	MISC:github.com/PoorlyNautilus/Security

SchoolCMS_File_Upload_Vuln · Issue #3 · PearlyNautilus/SchoolCMS · GitHub

Exploit
Third Party Advisory
github.com
text/html

MISC github.com/PearlyNautilus/Security-Code-Review/issues/3

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schoolcms	Schoolcms	2.3.1	All	All	All
Application	Schoolcms	Schoolcms	2.3.1	All	All	All

cpe:2.3:a:schoolcms:schoolcms:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:schoolcms:schoolcms:2.3.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→