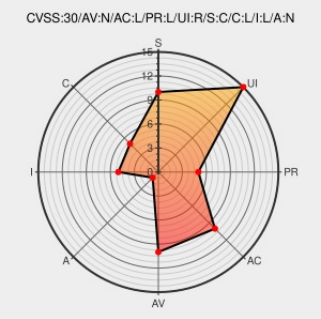
CVE-2017-9441

Published on: 06/05/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:50:00 AM UTC

CVE-2017-9441

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



Certain versions of Bigtree Cms from Bigtreecms contain the following vulnerability:

** DISPUTED ** Multiple cross-site scripting (XSS) vulnerabilities in BigTree CMS through 4.2.18 allow remote authenticated users to inject arbitrary web script or HTML by uploading a crafted package, triggering mishandling of the (1) title or (2) version or (3) author_name parameter in manifest.json. This issue exists in core\admin\modules\developer\extensions\install\unpack.php and core\admin\modules\developer\packages\install\unpack.php. NOTE: the vendor states "You must implicitly trust any package or extension you install as they all have the ability to write PHP files."

CVE-2017-9441 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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
Cross-site Scripting (XSS) in bigtreecms 4.2.18 · Issue #290 · bigtreecms/BigTree-CMS · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/bigtreecms/BigTree-CMS/issues/290

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bigtreecms	Bigtree Cms	All	All	All	All

cpe:2.3:a:bigtreecms:bigtree_cms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→