



CVE-2017-9364

Published on: 06/02/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9364

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

Certain versions of [Bigtree Cms](#) from [Bigtreecms](#) contain the following vulnerability:

Unrestricted File Upload exists in BigTree CMS through 4.2.18: if an attacker uploads an 'xxx.pht' or 'xxx.phtml' file, they could bypass a safety check and execute any code.

CVE-2017-9364 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Disabling phtml/pht files from being uploaded. · bigtreecms/BigTree-CMS@b722939 · GitHub	Patch github.com text/html	CONFIRM github.com/bigtreecms/BigTree-CMS/commit/b72293946951cc650eaf51f5d2f62ceac6335e12
Security hole for upload file bypass · Issue #280 ·	Exploit	CONFIRM github.com/bigtreecms/BigTree-

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	Bigtreecms	Bigtree Cms	All	All	All	All
cpe:2.3:a:bigtreecms:bigtree_cms:*:*:*:*:*:						

No vendor comments have been submitted for this CVE