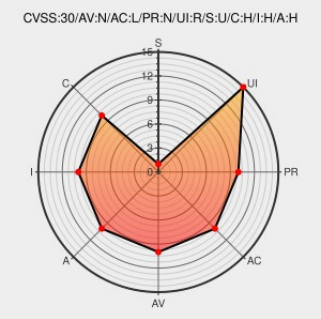
CVE-2017-7881

Published on: 04/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:40 PM UTC

CVE-2017-7881

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



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

BigTree CMS through 4.2.17 relies on a substring check for CSRF protection, which allows remote attackers to bypass this check by placing the required admin/developer/ URI within a query string in an HTTP Referer header. This was found in core/admin/modules/developer/_header.php and patched in core/inc/bigtree/admin.php on 2017-04-14.

CVE-2017-7881 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Updating PHPMailer to a more secure version, updating less.php to lat… · bigtreecms/BigTree-	Issue Tracking Patch	MISC github.com/bigtreecms/BigTree-CMS/commit/7761481ac40d83ac29fef42bc6b3c07c86694b56

CMS@7761481 · GitHub	Third Party Advisory github.com text/html	
BigTree CMS - Bypass CSRF filter and execute code with PHPMailer - cdxy	Exploit Third Party Advisory www.cdxy.me text/html	MISC www.cdxy.me/?p=765

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

← Previous ID

Next ID→

© CVE.report 2023 | |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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