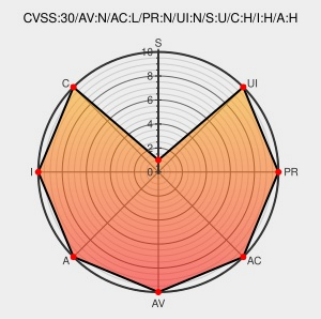
CVE-2016-6195

Published on: 08/30/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-6195

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



Certain versions of Vbulletin from Vbulletin contain the following vulnerability:

SQL injection vulnerability in forumrunner/includes/moderation.php in vBulletin before 4.2.2 Patch Level 5 and 4.2.3 before Patch Level 1 allows remote attackers to execute arbitrary SQL commands via the postids parameter to forumrunner/request.php, as exploited in the wild in July 2016.

CVE-2016-6195 has been assigned by 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
Security Update for vBulletin 4 - vBulletin.org Forum	Vendor Advisory www.vbulletin.org text/html	CONFIRM www.vbulletin.org/forum/showthread.php?t=322848

vBulletin CVE-2016-6195 SQL Injection Vulnerability	cve.report (archive) text/html	BID 92687
GitHub - drewlong/vbully: 3.8.x - 4.2.3 ForumRunner (vBulletin) exploit made easy.	github.com text/html	MISC github.com/drewlong/vbully
vBulletin <= 4.2.3 SQL Injection – enumerated	Technical Description Third Party Advisory enumerated.wordpress.com text/html	MISC enumerated.wordpress.com/2016/07/11/1/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vbulletin	Vbulletin	4.2.3	All	All	All
Application	Vbulletin	Vbulletin	4.2.3	All	All	All
Application	Vbulletin	Vbulletin	All	patch_level_4	All	All

cpe:2.3:a:vbulletin:vbulletin:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:*:patch_level_4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→