

CVE-2020-17496

vBulletin PHP Module Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

vBulletin 5.5.4 through 5.6.2 allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request. NOTE: this issue exists because of an incomplete fix for CVE-2019-16759.

EVRS 84 /100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.875 99.76th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
---	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.875 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vbulletin	≥ 5.5.4 ≤ 5.6.2	after 5.6.2	NVD

Sources

Vendor guidance	forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4445227-vbulletin-5-6-0-5-6-1-5-6-2-security-patch	NVD	nvd.nist.gov/vuln/detail/CVE-2020-17496
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-9444
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-17496		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.