



CVE-2020-7373

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-7373
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-30 17:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	vBulletin 5.5.4 through 5.6.2 allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbe

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Exploitee.rs » Blog Archive » Exploiting vBulletin: "A Tale of a Patch Fail"	MISC	blog.exploitee.rs
Full Disclosure: Remote Code Execution 0day in vBulletin 5.x	MISC	seclists.org
vBulletin 5.6.0, 5.6.1, 5.6.2 Security Patch - vBulletin Community Forum	MISC	forum.vbulletin.com
Vbulletin widget template rce by Zenofex · Pull Request #13970 · rapid7/metasploit-framework · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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 registered 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](#).

Free CVE JSON API cve.report/api

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