Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical vBulletin Flaws Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
June 4, 2025	A1	TA2025172

Summary

First Seen: May 23, 2025
Affected Products: vBulletin
Impact: Critical vulnerabilities, CVE-2025-48827 and CVE-2025-48828 have highlighted the serious risks of operating a public-facing vBulletin forum. These flaws, which are actively being exploited in the wild, enable attackers to gain full control of servers without authentication. To protect against such threats, site operators should urgently apply updates, limit access to administrative interfaces, and enforce robust security controls to minimize the risk of exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-48827	vBulletin Remote Code Execution Vulnerability	vBulletin	✗	✗	✓
CVE-2025-48828	vBulletin Remote Code Execution Vulnerability	vBulletin	✗	✗	✓

Vulnerability Details

#1 Two critical severity security vulnerabilities have been discovered in vBulletin, the popular forum software powering thousands of online communities. What makes this alarming is that these flaws tracked as CVE-2025-48827 and CVE-2025-48828 are already being actively exploited in the wild, putting both small forums and major platforms at risk.

#2 The first issue, CVE-2025-48827, affects installations running on PHP 8.1 or newer. It allows unauthenticated attackers to access and invoke protected API controller methods simply by crafting a malicious API request, like /api.php?method=protectedMethod. This essentially bypasses the expected access restrictions.

#3 The second flaw, CVE-2025-48828, targets the platform's template engine. By exploiting how vBulletin handles PHP function calls, attackers can craft template code using alternative syntax for example, "var_dump"("test") — to bypass filters and execute arbitrary PHP code. This abuse is made possible through PHP's Reflection API, which vBulletin misuses, especially under PHP 8.1.

#4 These flaws were exploited in the wild despite patches being quietly released back in April 2024. While a fix technically existed, it lacked public disclosure or CVE assignment at the time, making this a case of exploitation via undocumented patching. If you're running vBulletin, patching immediately or upgrading to the latest version is important. Leaving these flaws unpatched could leave your entire forum open to attack.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-48827	vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*:*:*	CWE-424
CVE-2025-48828	vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*:*:*	CWE-424

Recommendations

Update Immediately: If you're using vBulletin, the most important step is to update to the latest patched version as soon as possible. These bugs are already being exploited, so staying on an outdated version leaves your forum wide open to attack.

Restrict Public Access to API Endpoints: Limit access to the /api.php endpoint and other sensitive areas. If your forum doesn't need public API access, consider disabling it entirely or putting it behind authentication.

Use Web Application Firewalls (WAFs): Deploy a WAF or use server-level security tools that can block or flag unusual requests, such as attempts to access internal API functions or execute unauthorized PHP code.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	195[.]3[.]221[.]137, 169[.]150[.]203[.]14, 23[.]162[.]40[.]123, 176[.]65[.]149[.]193

Patch Details

Update your vBulletin to the latest version to address the flaws.
vBulletin 6.0.3 Patch Level 1
vBulletin 6.0.2 Patch Level 1
vBulletin 6.0.1 Patch Level 1
vBulletin 5.7.5 Patch Level 3

Link:
https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com

References

https://karmainsecurity.com/dont-call-that-protected-method-vbulletin-rce

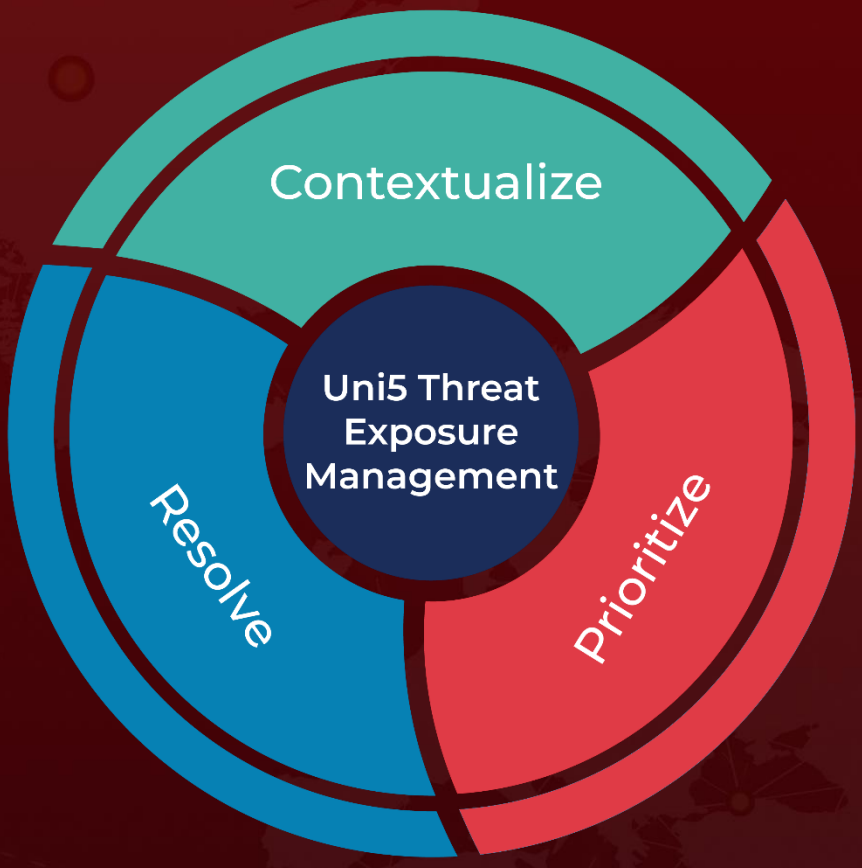
https://blog.kevintel.com/vbulletin-replaceadtemplate-kev/

https://isc.sans.edu/diary/vBulletin+Exploits+CVE202548827+CVE202548828/32006/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 4, 2025 • 6:00 AM

More at www.hivepro.com