Public Exploit Released for Critical vBulletin Remote Code Execution Vulnerability

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A public proof-of-concept exploit is available for CVE-2026-61511, a critical vulnerability affecting self-hosted vBulletin installations.

An unauthenticated attacker could exploit the vulnerability to remotely execute PHP code and operating system commands on an affected server.

Overview

There is a critical vulnerability (CVE-2026-61511, CVSS 9.8) in vBulletin that allows an unauthenticated attacker to remotely execute PHP code on an affected server. vBulletin is used to operate online forums, community websites and customer support portals.

An attacker could exploit improper input filtering in the template engine by sending a malicious request to the public `ajax/render/pagenav` route. Successful exploitation could expose forum data, allow operating system command execution and lead to malware or backdoor deployment.

Affected Products

- vBulletin 5.0.0 through 5.7.5
- vBulletin 6.0.0 through 6.2.1

***Note**: vBulletin 6.2.2 is not affected.*

vBulletin fixed the vulnerability in version 6.2.2 and patched its cloud environments. Although active exploitation has not been confirmed, unpatched self-hosted servers are at greater risk now that exploit code is publicly available.

Aspire Protects

- **Patch** - Upgrade self-hosted vBulletin installations to version 6.2.2 or later. Please see vBulletin's security advisory for more details.
- Migrate unsupported vBulletin 5.x installations to a patched 6.x version.
- Identify internet-facing installations and verify their versions.
- If patching must be delayed, temporarily block external access to the vulnerable `ajax/render/pagenav` route using a WAF or reverse proxy.
- Detection - Review web server, WAF and reverse-proxy logs for:
  - POST requests containing `routestring=ajax/render/pagenav`

- Unusually long or operator-heavy `pagenav[pagenumber]` values
- Commands or child processes launched by PHP or the web server
- New or modified PHP files, including web shells
- Unauthorized administrator activity
- Unusual outbound connections from the server
  - These patterns are based on the public PoC. They may indicate an exploitation attempt but do not confirm that the server was compromised.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – An attacker may exploit CVE-2026-61511 through a publicly accessible vBulletin template-rendering endpoint to execute PHP code without authentication.

Execution

- Command and Scripting Interpreter [T1059] – An attacker may use the vulnerability to execute PHP code and operating system commands in the context of the vBulletin web application.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerability may affect any organization operating an internet-facing, self-hosted vBulletin forum, including:

- Government
- Defense
- Technology
- Healthcare
- Telecommunications
- Finance
- Education
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

POC Released for Critical vBulletin Vulnerability

Security Patch Released for vBulletin 6.2.1, 6.2.0 and 6.1.6 - vBulletin Community Forum