

Critical WordPress Plugin Flaw CVE-2026-85097 Under Active Exploitation



A maximum-severity vulnerability in the Bricksforge WordPress plugin is being actively exploited, allowing unauthenticated attackers to execute arbitrary code remotely.

- CVE-2026-85097 carries a CVSS score of 10.0, the maximum severity rating
- The flaw affects the Bricksforge plugin for WordPress installations
- Attackers can upload and execute arbitrary PHP code without authentication
- Active exploitation has been confirmed by Patchstack researchers
- The vulnerability enables full remote code execution on vulnerable sites

Vulnerability Details

A critical security vulnerability designated **CVE-2026-85097** has been identified in the Bricksforge plugin for WordPress and is now under active exploitation. The flaw has been assigned the maximum Common Vulnerability Scoring System (CVSS) score of 10.0, reflecting its severe impact potential. According to security researchers at Patchstack, the vulnerability permits unauthenticated attackers to upload and execute arbitrary PHP code on affected WordPress installations.

Attack Mechanism

The vulnerability enables **remote code execution** (RCE) without requiring any form of authentication. This means attackers can gain complete control over vulnerable WordPress sites by exploiting the flaw to upload malicious PHP files and execute them on the target server. The unauthenticated nature of the exploit significantly lowers the barrier for attackers, as no credentials or prior access to the system are required.

Active Exploitation Confirmed

Patchstack has confirmed that threat actors are actively exploiting this vulnerability in real-world attacks. Organizations running WordPress installations with the Bricksforge plugin face immediate risk of compromise, potentially leading to data breaches, website defacement, malware distribution, or use of compromised servers as pivot points for further attacks within network environments.

What to do now

1. Immediately identify all WordPress installations within your organization's infrastructure and check for the presence of the Bricksforge plugin
2. Disable or remove the Bricksforge plugin from all WordPress sites until a security patch is available and tested
3. Review web server logs for suspicious PHP file uploads or execution attempts targeting WordPress installations
4. Implement web application firewall (WAF) rules to block unauthenticated file upload attempts to WordPress plugin directories
5. Conduct forensic analysis on any WordPress sites running Bricksforge to detect potential compromise indicators
6. Update incident response procedures to include WordPress plugin vulnerability management and coordinate with your web development teams on secure plugin vetting processes