ERT Threat Alert
New WordPress DoS Vulnerability
Feb 12, 2018

Abstract

On February 5, 2018, an independent researcher disclosed a zero-day vulnerability in WordPress that allows application-level denial-of-service (AppDoS) attacks against websites using the WordPress platform. WordPress is an open source content management system (CMS) written in PHP and powers over 29% of the Internet's sites and blogs.

The vulnerability (CVE-2018-6389) allows remote attackers to impact the performance and availability of any website leveraging WordPress. Attackers only require a single connected system with limited resources and bandwidth to inflict performance issues all the way up to website unavailability.

Attack Methods

WordPress uses a feature to reduce the amount of requests sent from a client browser to the server while loading JS (JavaScript) or CSS (Cascading Style Sheet) modules. The JS modules are required for core functionality while CSS provides the presentation description of the website. The feature is located under https://WPServer/wp-admin and is accessible without authentication. The load-scripts.php function was primarily designed for the admin pages of WordPress but is used also by the wp-login.php page; by consequence authentication cannot be enforced on the load-scripts.php url without breaking the functionality of the site.

Using a single request to https://WPServer/wp-admin/load-scripts.php an attacker can retrieve up to 181 JS modules from the server resulting in 181 file requests and almost 4MB of data transferred from the webserver to the client.

Using only a few lines of code, an attacker can easily launch concurrent requests and impact performance or bring down the site by consuming the server's CPU or saturating the outbound bandwidth.

Attackers can also leverage this technique for low and slow attacks, affecting CPU and consuming bandwidth over longer periods of time that could ultimately lead to higher bills at the end of the month for hosted sites that have contractual caps on CPU and/or bandwidth utilization. These low and slow attacks will go unnoticed until it is too late and are hard to identify without extra measures or alerting tools monitoring the abuse of the load-scripts.php page.

Targets

At the time of publication, Radware is only aware of a few dozen isolated exploit attempts. Since the vulnerability is now publicly disclosed and will remain unpatched, Radware considers this vulnerability to be critical for ensuring availability of WordPress-based websites. The vulnerability is easily exploited and it is possible that an increase in DoS and ransom DoS campaigns targeting WordPress-based sites will happen.

How to Prepare

DoS vulnerabilities are not in the scope of the bug bounty program provided by WordPress. The vulnerability was not considered as a bug or for future improvement by WordPress developers. WordPress' official statement was "This kind of thing should really be mitigated at the server or network level rather than the application level, which is outside of WordPress's control."

The discoverer of the vulnerability provides a forked WordPress project that includes a patch for the vulnerability without breaking wp-login.php. Despite the efforts of Barak Tawily for providing a bash script and a forked version of the project, Radware advises against using any descendants or forks that

are not officially recognized by WordPress. Future bug fixes and improvements might not be timely provided through unofficial branches of the project and therefore should be avoided if possible.

Detection and mitigation algorithms prevent attacks from scripts and automated tools without impacting good bots. Behavior algorithms are continuously monitoring and profiling individual client's actions and are able to detect and mitigate abuse from malicious users that might try to manually exploit the vulnerability through repeatedly requesting the offending URL.

Effective Web Application Security Essentials

To prevent this vulnerability from being exploited a Web Application Firewall is required that leverages advanced bot detection and mitigation algorithms that detect and block malicious scripts and automated tools without applying any penalty on 'good' bots. Users that might try to exploit the vulnerability manually by repeatedly requesting the offending URL will be blocked. This dynamic profile of application-traffic behavior yields an accurate anomaly detection of zero-day attacks.

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.