Nearly 7K WordPress Sites Compromised by Balada Injector

Dark Reading Staff
January 17, 2024

1 Min Read

Source: Primakov via Shutterstock

About 6,700 WordPress websites have been infected with the Balada Injector malware, after using a Popup Builder plug-in with a cross-site scripting (XSS) vulnerability tracked as CVE-2023-6000.

The Balada Injector campaign is long-running (since 2017) and is an operation that has compromised more than 1 million WordPress sites in the past six years. In the attack, a backdoor is injected to redirect visitors from a legitimate WordPress site to fake support pages and compromised or scam websites.

The threat actors in the most recent wave of activity exploited the XSS vulnerability to take over Popup Builder's "sgpbWillOpen" event and clear the way for malicious JavaScript code injection after the launch of a popup. Threat actors executed the JavaScript code by making changes to the "wp-blog-header.php" file.

This vulnerable version of the Popup Builder plug-in has more than 200,000 installations, so more infections could be coming.

"Malicious WordPress plug-ins are generally tricky to combat as victims install them without knowledge that vulnerabilities could exist. Prolonged periods without updates leave any vulnerabilities unaddressed, allowing threat actors to exploit them, as is the case with this new Balada Injector," Pedro Marrucho, security researcher at Jscrambler, wrote in an emailed statement.

To mitigate the issue and minimize its risk, Marrucho recommended implementing an integrity monitoring solution "that could be used to keep track of threat actor activity on the website," as well as keeping third-party code involvement to a minimum and "performing routine updates on them."

About the Author(s)

Dark Reading Staff

Dark Reading

Dark Reading is a leading cybersecurity media site.

See more from Dark Reading Staff

Keep up with the latest cybersecurity threats, newly discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

Subscribe

You May Also Like