WordPress Server Compromise

Date: 2025-03-16
Handler: Jacob C.

Executive Summary

On 2021-02-04, an injection attack occurred targeting insecure WordPress plugins.
After a couple of attempts, the plugin “WordPress-gallery-plugin” was successfully attacked, and a malicious file, bbb.php, was attached to it. After tampering with this bbb.php file, the attacker was able to access parts of the server he shouldn’t have gotten access to. This then allowed another attacker to gain access to the admin panel of the WordPress page. Eventually, the attacker added his own content and overridded the owner's blog. The total financial impact is $300.

Timeline

2021-02-03 9:32 - An attacker tried accessing the xmlrpc.php and attempted a brute force attack to gain unauthorized access to the page until 9:42

2021-02-04 14:23 - An Attack began with a user trying to inject a malicious file named bbb.php into different plugins on the WordPress server. They were successful at appending this malicious file on the “WordPress-gallery-plugin” file.

2021-02-05 9:12 - An Attack with a different ip address began posting information to the bbb.php file. This occurred with byte sizes over 1231512 in length.

2021-02-05 9:14 - Another attacker from a different ip address is again targeting the bbb.php file.

2021-02-05 18:12 - A potentially malicious user is trying to access the backup configuration file for WordPress but doesn’t succeed

2021-02-05 15:56 - A potentially malicious user is accessing the xmlrpc file and posting to it

2021-02-06 23:39 - Another user is posting information in the bbb.php file. A couple of minutes later, they were successfully able to access the admin page, most likely due to exploits within the bbb.php file.

2021-02-6 23:41 - The same user begins to make several edits and changes to the admin panel, which allows them to change the website however they want.

2021-02-06 23:46 - The attacker makes his last post request, which leaves the new webpage with the attacker's advertised essays.

Containment and eradication steps

On 2021-02-03, when the brute force attack occurred, I blocked that IP address and talked to the owner about adding automated IP blocking. In addition, I disabled the xmlrpc file due to its vulnerabilities

The next day, we noticed the plugins getting attacked, and the gallery plugin was injected with the bbb.php file. We completely shut down the server and removed the gallery plugin. After this, we made sure the other plugins didn't have any other vulnerabilities and reset the server from a backup.

Financial Impact

Labor Costs: $30/hr = 30*10 = $300
Total cost: $300

Lessons Learned

Successes:

- The logs showed every action the attacker took, which allowed me to find the problem
- The brute force attack didn't work due to well-made passwords

Opportunities for Improvement:

- All plugins should be thoroughly inspected and researched to ensure they are secure without any vulnerabilities
- Malicious attackers should be immediately blocked and shouldn't be able to interact with the website
- Website traffic should be more closely monitored so responses to attacks are swift so only minimal damage will occur