Incident Report: WordPress Plugins

Date: 03/12/2025

Handler: Enrique Gonzalez-Esquivel

# Executive Summary:

A WordPress website hosted by SecureTech Solutions was compromised between Feb 3-6, 2021, which resulted in unauthorized access to admin controls and modification of the site’s content to promote cheap essay writing services. Began with probing, checked xmlrpc.php, then wp-login, and then tried user enumeration through /?author=1. Confirmed that ‘admin’ exists, they launched a brute force attack against xmlrpc.php. The attack appears to be a vulnerable WordPress gallery plugin (timthumb.php), a vulnerability that allows attackers to upload and execute arbitrary PHP code in the timthumb cache directory, leading to remote code execution. The attacker uploaded (bbb.php) through the vulnerable plugin and later modified the site’s content.

# Timeline:

[02/Feb/2021:13:38:59 -0500 - 03/Feb/2021:05:44:00 -0500] - Normal website operation with bot crawling from search engines.

[03/Feb/2021:09:32:40 -0500 - 03/Feb/2021:09:42:03 -0500] - Initial probing begins from IP 47.75.76.54, attacker attempts to access wp-login.php, performs WordPress username enumeration via /?author=1, identifies “admin” and launches brute force attack against xmlrpc.php(+100 POST requests)

[04/Feb/2021:14:23:08 -0500 - 04/Feb/2021:14:23:18 -0500] - New attacker (72.167.247.190) tries multiple WordPress plugins for vulnerabilities, identifies “wordpress-gallery-plugin” via timthumb.php vulnerability and upload bbp.php to the gallery plugin directory.

[06/Feb/2021:23:41:23 -0500 - 06/Feb/2021:23:46:04 -0500] - New Attacker (157.75.167.23) successfully logs into WordPress admin panel, modifies post ID1, changes content to advertise cheap essay writing services

# Actions Taken:

February 12, 2021, the security team should have been notified of suspicious activity on the website. Investigation confirms website compromise. Create backup. Website should've been taken offline to prevent damage. All WordPress admin passwords reset and forced logout of all sessions. Vulnerable “wordpress-gallery-plugin” removed and other plugins updated to latest versions. Check that all files are clean, ensuring no remaining malicious files. Once the adversary has been evicted from the environment and all known vulnerable paths have been eliminated, initiate restoration steps. Notify the customer of the security incident.

# Financial Impact:

Security analyst investigation ~16 hours @85/hr, Website downtime ~8hrs @ estimated $2,400, users notification(data potentially exposed) @ $1,200, reputations damage @$5,000 (estimated on customer trust impact, Security improvements, update monitoring setup and security staff awareness training @ $7,800. Total cost ~ $17,760.

# Lessons Learned:

Plugin management: moving forward the goal is to implement a process for evaluating WordPress plugins. Also removing unused or unnecessary plugins. Deploying a WAF that is specifically configured to block common attack patterns like xmlrpc.php abuse and plugin exploitation attempts. Furthermore, implement monitoring to detect unauthorized file changes to the WordPress installation. Lastly, implementing requirements for third-party plugins, that includes a security review before installation.

## Successes:

Database integrity, the core database structure remained intact. Authentication functionality worked properly, as the attacker needed to use alternative methods such as exploitation of a vulnerable plugin rather than directly bypassing authentication. Lastly, the incident provides clear evidence that can now be used to improve security and detection capabilities.

## Opportunities for Improvement:

Conduct security awareness training that focuses on WordPress security for all website administrators. Also consider a dashboard to monitor specific WordPress installations to help improve detection capabilities. Implement a staging environment for updates before applying them to production. Also focus on input validation and brute force protection, like limiting login attempts, CAPTCHA implementation and even IP-based access control.

### 

### 

### Resources:

<https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-containment-eradication-recovery>

<https://usa.kaspersky.com/blog/security_risks_report_financial_impact/>

<https://www.xcitium.com/blog/it-security/what-to-do-if-your-company-has-been-hacked/>

<https://www.hostinger.com/tutorials/xmlrpc-wordpress>

<https://blog.sucuri.net/2019/08/timthumb-attacks-the-scale-of-legacy-malware-infections.html>