Wordpress Incident Response

## Date: 2021--02-12

## Handler: Noah Scott

# Executive Summary

On 2021-02-10 at 9:00 AM PST, I received an urgent ticket from one of our clients who claimed their online blog had been compromised post “installing WordPress and some plugins.” Upon investigation, I found that several attacks were taking place due to some insecure settings and plugins on this WordPress site. One attacker was utilizing the insecurities of XML-RPC to brute-force logging into the user account “admin.” XML-RPC is known to allow multiple login attempts without locking a user out for failed logins. There was also an indication of another user successfully logging into the admin account using a known vulnerability with the TimThumb plugin.

TimThumb is a script used on WordPress for resizing images that is included in various WordPress plugins. In our situation, the WordPress Gallery Plugin is outdated and contains an outdated version of TimThumb, which is vulnerable to arbitrary file uploads.

This led to the attacker uploading an unknown PHP script labeled “bbb,” which allowed them to gain access to the admin account. With admin account access, they did some “ducking,” which eventually led to the site being infected with essay help spam.

# Background

The website in question is a blog post website. The client claimed to have installed WordPress, so I would assume the site wasn’t originally a WordPress site. They also claimed to have installed some WordPress plugins, which could be problematic.

WordPress is a free, open-source content management system that grants users the ability to create and manage websites. It is a commonly used CMS; however, it comes with some possible vulnerabilities related to the use of outdated plugins and misconfigured settings.

# Timeline

2021-02-02 at 10:38 AM PST - Attackers begin recon of website

2021-02-03 at 6:32 AM PST – Attacker found valid username and began brute forcing (825 attempts)

2021-02-03 at 6:42 AM PST – Brute force attack on xml-rpc ends with no sign of a login

2021-02-04 at 11:23 AM PST – An attacker exploits timthumb and uploads “bbb.php”

2021-02-05 at 9:12 AM PST – The attacker continues to make requests to the endpoint containing the newly uploaded script. Each one returns a large amount of data.

2021-02-06 at 5:39 PM PST – Attacker with a different IP starts making requests to the bbb.php script again and then tries to login but appears to be logged out.

2021-02-06 at 5:40 PM PST - Account “admin2” is created

2021-02-06 at 5:41 PM PST – Attacker accesses the load styles endpoint and floods the parameters resulting in a return in a large amount of data. User is logged into the admin at this point and begins to deface the logs and the site.

2021-02-10 at 9:00 AM PST - Owner of this website contacted me to make an incident report.

# Findings

On February 2, 2021, at 10:38 AM PST, the attacker began reconnaissance on the website. Logs show that an automated bot, possibly a search engine crawler, accessed various pages, including robots.txt, which may have revealed sensitive directories that were not meant for public indexing.

On February 3, 2021, at 6:32 AM PST, the attacker identified a valid username and initiated a brute force attack against the WordPress xmlrpc.php endpoint, attempting 825 login requests in a short period. The attack continued for approximately ten minutes but may have failed to gain access.

On February 4, 2021, at 11:23 AM PST, the attacker successfully exploited a known vulnerability in TimThumb, a WordPress image resizing script, to upload a PHP backdoor (bbb.php). This suggests the website was running an outdated and vulnerable version of the plugin.

On February 5, 2021, at 9:12 AM PST, the attacker began making repeated requests to the endpoint containing bbb.php. Each request returned a large amount of data, indicating possible data exfiltration or reconnaissance of the server environment.

On February 6, 2021, at 5:39 PM PST, a new attacker with a different IP address began making requests to bbb.php, suggesting collaboration or the sale of access to a third party. Shortly after, an unauthorized admin account ("admin2") was created, possibly indicating a successful privilege escalation.

At 5:41 PM PST on the same day, the attacker accessed the WordPress style endpoint and manipulated parameters to flood the system, likely leveraging a form of denial-of-service (DoS) attack or data extraction technique. At this point, the attacker had full administrative access and began altering site logs and defacing the website.

On February 10, 2021, at 9:00 AM PST, the website owner discovered the incident and requested an investigation, suggesting that the attack remained undetected for several days.

# Actions Taken

Due to XML-RPC being exploited, I disabled it in the .htaccess file, as it seemed unnecessary for the client’s needs. Next, I changed the admin password, as it was most likely leaked during the attack, and removed the second admin account labeled "admin2."

The TimThumb vulnerability is tied to CVE-2011-4106. This CVE states that TimThumb versions older than 2.0 allow the upload and remote execution of arbitrary files, such as the bbb.php script found in the logs. With that in mind, I uninstalled all plugins to eliminate any other potential vulnerabilities from the site.

It would be wise to check for plugin vulnerabilities before installing them. Establishing a checks-and-balances system when adding new features to the website would help mitigate potential exploits caused by human error.

Next, I ensured that the server directory hosting the site follows the principle of least privilege to restrict access and reduce the risk of further exploitation.

# Financial Impact

| Item | Cost |
| --- | --- |
| Investigation Cost | $2,000 |
| Security Consultant Fees | $6,000 |
| Immediate Mitigation Expenses | $5,000 |
| Downtime Impact | $5,000 |
| Reputation Damage | $10,000 |
| Regulatory Fines & Legal Penalties | $10,000(est) |
| Total | $38,000 |

1. 40 hours at a rate of $50 per hour = Investigation Cost ($2,000)
2. 20 hours at a rate of $300 per hour = Security Consultant Fees ($6,000)
3. Estimated cost for patching, plugin removal, WordPress updates, and security hardening = Immediate Mitigation Expenses ($5,000)
4. 3 business days of downtime at an estimated loss of $5,000 = Downtime Impact ($5,000)
5. Estimated loss due to customer distrust and reduced traffic = Reputation Damage ($10,000)
6. Placeholder estimate for potential regulatory penalties = Regulatory Fines & Legal Penalties ($10,000 est.)

# Lessons Learned

## Successes

* The access logs provided great detail and were successful in helping me find key weaknesses.

## Opportunities for Improvement

**Issue: Wordpress plugins (timthumb)**

**Recommendation:** Use only up to date plugins that offer regular patches.

**Action Item Owner:** Website owner

**Issue: XML-RPC**

**Recommendation:** Disable xml-rpc on the site if not necessary to prevent brute force and security bypass atempts

**Action Item Owner:** Website owner