

Investigation Report – Compromised WordPress

This investigation identified a successful Remote Code Execution (RCE) attack against a WordPress installation. The attack chain involved exploitation of known vulnerabilities in two plugins (*Contact Form 7* and *Simple File List*), leading to the unauthorized upload and execution of a malicious web shell.

Findings

- **Timeframe:** 2021-01-14 05:42:34 – 06:30:11 UTC
- **Host:** 172.21.0.3 (WordPress webserver)
- **IOC IPs:**
 - 119.241.22.121 (Japan)
 - 103.69.55.212 (Taiwan)
- **Vulnerable Plugins:**
 - simple-file-list (v4.2.2)
 - contact-form-7 (v5.3.1)
- **Malicious File:** fr34k.png > executed as fr34k.php
- **Attack Type:** Remote Code Execution (RCE) via plugin vulnerability
- **Confirmed Impact:** Successful upload and execution of a web shell

Investigation Summary

On January 14th, 2021, a WordPress server (172.21.0.3) was compromised through exploitation of a known vulnerability in the simple-file-list plugin (versions <= 4.2.2). The attacker began by performing reconnaissance on the site, identifying exposed plugins and configurations using WPScan and path traversal attempts.

The actor then exploited the plugin to upload a malicious file named fr34k.png, which was a web shell disguised as an image. Shortly after uploading, the same file was accessed at fr34k.php, confirming successful execution of the shell.

Two external IP addresses (Japan and Taiwan) were involved, suggesting either collaboration or the use of a proxy/VPN.

After the compromise, no further activity was observed in the logs.

Who, What, When, Where, Why, How

Who:

- Threat actor(s) using IPs 119.241.22.121 (Japan) and 103.69.55.212 (Taiwan).
- Likely automated exploitation tools or proxy/VPN use.

What:

- Multi-stage attack leading to Remote Code Execution (RCE) on a WordPress host.
- Attacker uploaded and executed a web shell (fr34k.php).

When:

- January 14th, 2021, between 05:42:34 UTC - 06:30:11 UTC.
- No evidence of ongoing activity after this window.

Where:

- Targeted WordPress environment at internal host 172.21.0.3.
- Exploited components: simple-file-list and contact-form-7 plugins.

Why:

- Motives are likely to gain unauthorized remote access. Possibly for persistence, data theft, or use as a launchpad for further attacks.

How:

1. **Reconnaissance (05:42:34):**
Scanning plugin paths and themes (crawling activity).
2. **Discovery (05:54:14):**
Tested login tokens via /wp-login.php using parameter itsec-hb-token=adminlogin.
3. **Scanning (06:01:41):**
WPScan enumeration to detect vulnerable plugins.
4. **Exploitation (06:26:53):**
Used Simple File List RCE vulnerability to upload fr34k.png.
5. **Execution (06:30:11):**
File accessed as fr34k.php from 103.69.55.212, confirming shell execution.

Recommendations

1. Preserve and contain the affected host (172.21.0.3) by creating a full system snapshot for forensic review. Keep the site online behind a Web Application Firewall (WAF) to block further exploit attempts while investigation continues.
2. Identify and remove malicious artifacts. Specifically, the uploaded web shell fr34k.php (originally fr34k.png) and reset all WordPress, database, and FTP credentials to prevent re-entry.
3. Update and harden the environment: patch or remove the vulnerable plugins (simple-file-list, contact-form-7), apply all WordPress updates, and enable centralized logging and monitoring to detect similar activity in the future.