Wordfence
Unauthenticated XSS Vulnerability
Patched in HTML Email Template
Designer Plugin

Chloe Chamberland

January 19, 2022

Unauthenticated XSS Vulnerability Patched in HTML Email Template Designer Plugin

On December 23, 2021 the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerability we discovered in “WordPress Email Template Designer – WP HTML Mail”, a WordPress plugin that is installed on over 20,000 sites. This flaw made it possible for an unauthenticated attacker to inject malicious JavaScr that would execute whenever a site administrator accessed the template editor. This vulnerability would also allow th to modify the email template to contain arbitrary data that could be used to perform a phishing attack against anyon who received emails from the compromised site.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on December 23, 2021. Sites still using the free version of Wordfence will receive the same protection on January 22, 20

We sent the full disclosure details to the developer on January 10, 2022, after multiple attempts to contact the develo and eventually receiving a response. The developer quickly acknowledged the report and released a patch on Januar 13, 2022.

We strongly recommend ensuring that your site has been updated to the latest patched version of “WordPress Email Template Designer – WP HTML Mail”, which is version 3.1 at the time of this publication.

Description: Unprotected REST-API Endpoint to Unauthenticated Stored Cross-Site Scripting and Data Modification
Affected Plugin: WordPress Email Template Designer – WP HTML Mail
Plugin Slug: wp-html-mail
Plugin Developer: codemiq
Affected Versions: <= 3.0.9
CVE ID: CVE-2022-0218
CVSS Score: 8.3 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1

WP HTML Mail is a WordPress plugin developed to make designing custom emails simpler for WordPress site owner

Unfortunately, these were insecurely implemented making it possible for unauthenticated users to access these endpoints.

More specifically, the plugin registers the `/themesettings` endpoint, which calls the `saveThemeSettings` function or `getThemeSettings` function depending on the request method. The REST-API endpoint did use the `permission_callback` function, however, it was set to `__return_true` which meant that no authentication was requ to execute the functions. Therefore, any user had access to execute the REST-API endpoint to save the email's theme settings or retrieve the email's theme settings.

```php
public function rest_api_init() {
    register_rest_route( $this->api_base, '/themesettings', array(
        'methods' => 'GET',
        'callback' => [ $this, 'getThemeSettings' ],
        'permission_callback' => '__return_true'
    ));

    register_rest_route( $this->api_base, '/themesettings', array(
        'methods' => 'POST',
        'callback' => [ $this, 'saveThemeSettings' ],
        'permission_callback' => '__return_true'
    ));
}
```

As this functionality was designed to implement setting changes for the email template, an unauthenticated user cou easily make changes to the email template that could aid in phishing attempts against users that receive emails fron the targeted site. Worse yet, unauthenticated attackers could inject malicious JavaScript into the mail template that would execute anytime a site administrator accessed the HTML mail editor.

As always, cross-site scripting vulnerabilities can be used to inject code that can add new administrative users, redire victims to malicious sites, inject backdoors into theme and plugin files, and so much more. Combined with the fact tl the vulnerability can be exploited by attackers with no privileges on a vulnerable site, this means that there is a high chance that unauthenticated attackers could gain administrative user access on sites running the vulnerable version the plugin when successfully exploited. As such, we strongly recommend that you verify that your site is running the most up to date version of the plugin immediately.

Timeline

December 23, 2021 – Conclusion of the plugin analysis that led to the discovery of a Stored Cross-Site Scripting Vulnerability in the "WordPress Email Template Designer – WP HTML Mail" plugin. We develop and release a firewall to protect Wordfence users. Wordfence Premium users receive this rule immediately. We attempt to initiate contact v the developer.
January 4, 2022 – We send an additional outreach attempt to the developer.
January 10, 2022 – The developer confirms the inbox for handling the discussion. We send over the full disclosure details.
January 11, 2022 – The developer acknowledges the report and indicates that they will work on a fix.
January 13, 2022 – A fully patched version of the plugin is released as version 3.1.
January 22, 2022 – The firewall rule becomes available to free Wordfence users.

Conclusion

In today's post, we detailed a flaw in the "WordPress Email Template Designer – WP HTML Mail" plugin that made it possible for unauthenticated attackers to inject malicious web scripts that would execute whenever a site owner accessed the mail editor area plugin, which could lead to complete site compromise. This flaw has been fully patche version 3.1.

We recommend that WordPress site owners immediately verify that their site has been updated to the latest patchec version available, which is version 3.1 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on December 22, 2021. Sites still using the free version of Wordfence will receive the same protection on January 22, 20

them to help keep their sites protected as this is a serious vulnerability that can lead to complete site takeover.

If your site has been compromised by an attack on this or any other plugin, our Professional Site Cleaning services ca help you get back in business.

Did you enjoy this post? Share it!

Comments

No Comments

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service Privacy Policy

CCPA Privacy Notice

Products

Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence Central

Support

Documentation
Learning Center
Free Support
Premium Support

News

Blog
In The News
Vulnerability Advisories

About

About Wordfence
Careers
Contact
Security
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

□ By checking this box I agree to the terms of service and privacy policy.*