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

WordPress plugin flaw puts users of 20,000 sites at phishing risk

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

January 20, 2022 10:50 AM **0**

The WordPress WP HTML Mail plugin, installed in over 20,000 sites, is vulnerable to a high-severity flaw that can lead to code injection and the distribution of convincing phishing emails.

'WP HTML Mail' is a plugin used for designing custom emails, contact form notifications, and generally tailored messages that online platforms send to their audience.

The plugin is compatible with WooCommerce, Ninja Forms, BuddyPress, and others. While the number of sites using it isn't large, many have a large audience, allowing the flaw to affect a significant number of Internet users.

Top Articles
MAERSK LINE
READ MORE
(https://www.bleepingcomputer.com/news/security/phishing-impersonates-shipping-giant-maersk-to-push-strrat-malware/?traffic_source=Connatix)
Phishing impersonates shipping giant Maersk to push STRRAT malware

According to a report by Wordfence's Threat Intelligence team, an unauthenticated actor could leverage the flaw tracked as "CVE-2022-0218" to modify the email template to contain arbitrary data of the attacker's choosing.

Additionally, threat actors can use the same vulnerability to send phishing emails to anyone registered on the compromised sites.

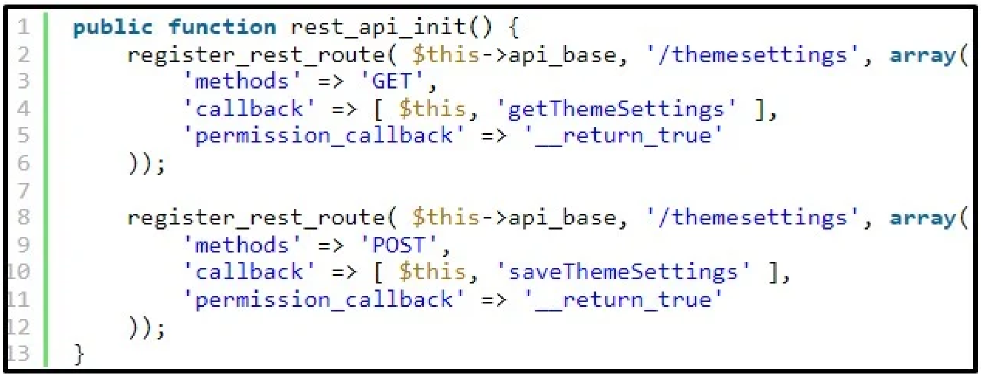
Unprotected API endpoints

The problem lies in the plugin's registration of two REST-API routes used to retrieve and update email template settings.

These API endpoints aren't adequately protected from unauthorized access, so even unauthenticated users can call and execute the functions.

As Wordfence explains in detail in its report (https://www.wordfence.com/blog/2022/01/unauthenticated-xss-vulnerability-patched-in-html-email-template-designer-plugin/):

> *The plugin registers the /themesettings endpoint, which calls the saveThemeSettings function or the 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 required 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.*



```
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'
    ));
}
```

The two unprotected REST-APIs

Source: Wordfence

Apart from the possibility of phishing attacks, an adversary could also inject malicious JavaScript into the mail template, which would execute anytime the site administrator accessed the HTML mail editor.

This could potentially open the way to adding new admin accounts, redirect the site's visitors to phishing sites, inject backdoors into the theme files, and even complete site takeover.

Disclosure and fix

Wordfence discovered and disclosed the vulnerability to the plugin's developer on December 23, 2021, but they only got a response on January 10, 2022.

The security update that addressed the vulnerability came on January 13, 2022, with the release of version 3.1.