Chloe Chamberland

October 27, 2021

1,000,000 Sites Affected by OptinMonster Vulnerabilities

Note: To receive disclosures like this in your inbox the moment they're published, you can subscribe to our WordPress Security Mailing List.

On September 28, 2021 the Wordfence Threat Intelligence team initiated the responsible disclosure process for several vulnerabilities we discovered in OptinMonster, a WordPress plugin installed on over 1,000,000 sites. These flaws made it possible for an unauthenticated attacker, meaning any site visitor, to export sensitive information and add malicious JavaScript to WordPress sites, among many other actions.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on September 28, 2021. Sites still using the free version of Wordfence will receive the same protection on October 28, 2021.

We sent the full disclosure details to OptinMonster on September 28, 2021, after confirming the appropriate channel to handle communications.The OptinMonster team quickly acknowledged the report by releasing a patch the next day. We followed up to let them know some improvements were needed on the patch and a fully patched version was released as 2.6.5 on October 7, 2021.

We strongly recommend validating that your site has been updated to the latest patched version of OptinMonster which is 2.6.5 at the time of this publication.

Description: Unprotected REST-API to Sensitive Information Disclosure and Unauthorized app.optinmonster.com API access
Affected Plugin: OptinMonster
Plugin Slug: optinmonster
Affected Versions: <= 2.6.4
CVE ID: CVE-2021-39341
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.6.5

OptinMonster is an incredibly intuitive and easy to use plugin designed to create sales campaigns on WordPress sites through the use of dialogs. The vast majority of the plugin's functionality as well as the OptinMonster app site rely on the use of API endpoints to allow seamless integration and a streamlined design process.

Unfortunately, the majority of the REST-API endpoints were insecurely implemented, making it possible for unauthenticated attackers to access many of the various endpoints on sites running a vulnerable version of the plugin.

The most critical of the REST-API endpoints was the `/wp-json/omapp/v1/support` endpoint, which disclosed sensitive data like the site's full path on the server, along with the API key needed to make requests on the OptinMonster site. With access to the API key, an attacker could make changes to any campaign associated with a site's connected OptinMonster account and add malicious JavaScript that would execute anytime a campaign was displayed on the exploited site.

Worse yet, an attacker did not need to be authenticated to the site in order to access the API endpoint due to the functionality implemented within the `logged_in_or_has_api_key` function used as the `permissions_callback`. For instance, if a request to an API endpoint had the `Referer` header set to `https://wp.app.optinmonster.test` and the HTTP request type set to OPTIONS then the function would return `true` thereby passing the capability check. An attacker could simply meet these requirements and set the `X-HTTP-Method-Override` HTTP header to the method required for the REST-API endpoint, such as GET or POST, to successfully make the request.

```
1475  public function logged_in_or_has_api_key( $request ) {
1476      if (
1477          ! empty( $_SERVER['HTTP_REFERER'] )
1478          && false !== strpos( $_SERVER['HTTP_REFERER'], 'https://wp.app.optinmonster.test' )
1479          && 'OPTIONS' === $_SERVER['REQUEST_METHOD']
1480      ) {
1481          return true;
1482      }
1483
1484      return is_user_logged_in() || true === $this->has_valid_api_key( $request );
1485  }
```

This meant that any unauthenticated attacker could add malicious JavaScript to a site running OptinMonster, which could ultimately lead to site visitors being redirected to external malicious domains and sites being completely taken over in the event that JavaScript was added to inject new administrative user accounts or overwrite plugin code with a webshell to gain backdoor access to a site.

Fortunately, the OptinMonster team invalidated all API keys to force site owners to generate new keys in the off chance that a key had been previously compromised, and implemented restrictions that inhibited API keys associated with WordPress sites from being able to make campaign changes using the OptinMonster app which prevents successful exploitation of this vulnerability chain.

Not the Only Endpoint Affected

In addition to the `/wp-json/omapp/v1/support` endpoint, nearly every other REST-API endpoint registered in the plugin was vulnerable to authorization bypass due to insufficient capability checking allowing unauthenticated visitors, or in some cases authenticated users with minimal permissions, to perform unauthorized actions. Attackers could do things like change settings, view campaign data, enable/disable debug mode, and more.

Disclosure Timeline

September 28, 2021 6:07 PM UTC – Conclusion of the plugin analysis that led to the discovery of multiple vulnerabilities in the OptinMonster WordPress plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users.
September 28, 2021 6:12 PM UTC – We initiate contact with the plugin vendor asking that they confirm the inbox for handling the discussion.

September 28, 2021 6:19 PM UTC – The vendor confirms the inbox for handling the discussion.
September 28, 2021 7:06 PM UTC – We send over the full disclosure details.
October 7, 2021 – A fully patched version of the plugin, 2.6.5, is released.
October 28, 2021 – Wordfence free users receive the firewall rule.

Conclusion

In today's post, we detailed a flaw in the OptinMonster plugin that enabled a dangerous exploit chain which made it possible for unauthenticated attackers to retrieve a site's sensitive data and gain unauthorized access to OptinMonster user accounts, which could be used to add malicious scripts to vulnerable sites. These flaws have been fully patched in version 2.6.5.

We recommend that WordPress users immediately verify that their site has been updated to the latest patched version available, which is version 2.6.5 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on September 28, 2021. Sites still using the free version of Wordfence will receive the same protection on October 28, 2021.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as these are serious vulnerabilities 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 can help you get back in business.

Did you enjoy this post? Share it!

Comments

2 Comments

Predrag *
October 29, 2021
10:11 am

Hello,

What this actualy means?

"Fortunately, the OptinMonster team invalidated all API keys to force site owners to generate new keys in the off chance that a key had been previously compromised, and implemented restrictions that inhibited API keys associated with WordPress sites from being able to make campaign changes using the OptinMonster app which prevents successful exploitation of this vulnerability chain."

Does it mean that this vulnerability can't be exploited until the user generates new key from the admin panel?
Also, when did the plugin author invalidated Api keys?

Chloe Chamberland *
November 1, 2021
10:43 am

Hi there,

The API keys were reset so that in the off chance they were compromised prior to the vulnerability being patched, the vulnerability could no longer be exploited using an old API keys. We have no evidence that suggests these API keys were compromised, however, reseting the API keys makes sure there is no possibility for attackers to use these old keys. We are not sure the exact date these keys were invalidated, however, it occurred at some point over the past month. Thanks!