Chloe Chamberland

October 20, 2021

Vulnerability Patched in Sassy Social Share Plugin

Update: This article has been updated for accuracy: while we initially did create a rule to block this vulnerability we later found that the vulnerability was already blocked by an existing rule.

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

In 2010, Steffan Esser gave a presentation in Las Vegas that rocked the PHP world. He had discovered a new kind of vulnerability that today we call a "PHP Object Injection" vulnerability. This kind of vulnerability allows an attacker to send a PHP application some data that is turned into an object that lives in memory. If the application then assumes that object and its data is secure, and does things with that object, it could lead to a compromised website.

In technical terms, the way an object injection vulnerability works is as follows. A developer writes code that uses the `unserialize()` function. This function is a way to take an object that has been stored somewhere, and turn it from it's stored form, which looks like text, back into an object that lives in memory. Developers do this when using object oriented programming in PHP. Objects are just data structures that logically represent things within the application. The `serialize()` and `unserialize()` functions are ways to store and retrieve objects. While `serialize()` turns an object into text, ready for storage, `unserialize()` takes the text and turns it back into an object that you can use in the application.

What Steffan discovered is that many developers were assuming that their objects, once unserialized in memory, were safe. And if he could send malicious data to the unserialize function, that is later used by the application and assumed to be safe, he could gain remote code execution on a website or in any PHP application. He had discovered a whole new way to hack into many websites across the globe.

Today we are disclosing an object injection vulnerability in a popular WordPress plugin. This vulnerability allows an attacker to submit data that is unserialized by PHP, and could contain malicious data. This malicious data is used by code in the application that trusts that the data is safe, creating a vulnerability that allows an attacker to take over a WordPress website.

PHP Object Injection Vulnerability in Sassy Social Share

On August 31, 2021 the Wordfence Threat Intelligence team discovered a vulnerability in "Sassy Social Share", a WordPress plugin installed on over 100,000 sites. The vulnerability provided a way for subscriber level users to gain remote code execution and take over a vulnerable site. Sites that have open registration allow anyone to create a "subscriber" level account, and are particularly vulnerable to this vulnerability.

After developing a firewall rule to protect against exploits targeting this vulnerability on August 31, 2021, we determined that another rule provided sufficient protection and archived the original custom rule. Both free and premium Wordfence users have been protected against this vulnerability since it was introduced in version 3.3.23.

In this case, the flaw made it possible for an attacker to import plugin settings and potentially inject PHP Objects that could be used as part of a POP Chain – a code execution sequence in the application that is exploited by the attacker.

On August 31, 2021, we initiated the responsible disclosure process. The vendor responded the next day, on September 1, 2021 after which we sent over the full disclosure details.

After working with the developer over a couple of weeks, a patch was released on September 17, 2021 in version 3.3.24. As per our responsible disclosure policy, we are now disclosing the vulnerability details because the plugin has been fully patched for some time.

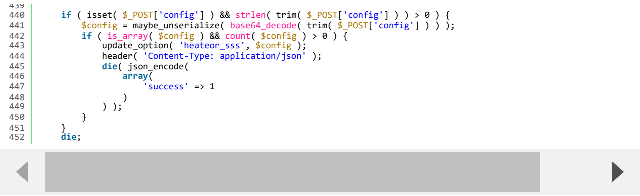
If you have not already done so, we strongly recommend updating to the latest patched version of Sassy Social Share, which is version 3.3.25 at the time of this publication, as soon as possible, especially if you are running the vulnerable version of the plugin, which is version 3.3.23.

Description: Missing Authorization Controls to PHP Object Injection
Affected Plugin: Sassy Social Share
Plugin Slug: sassy-social-share
Plugin Vendor: Team Heateor
Affected Versions: 3.3.23
CVE ID: CVE-2021-39321
CVSS Score: 6.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Researcher/s: Chloe Chamberland

Sassy Social Share is an easy to use plugin designed to enhance a site's social media presence. One of the plugin's recent updates introduced the ability to import and export the settings for the plugin. Unfortunately, this was insecurely implemented making it possible for authenticated users to import the plugin's settings along with arbitrarily injecting PHP objects.

In order to provide this functionality the plugin registered the `wp_ajax_heateor_sss_import_config` AJAX action which is hooked to the `import_config` function. Unfortunately, this function had no capability checks, nor any nonce protection which meant that any authenticated user could trigger the AJAX action.

In this vulnerability's simplest form it could be used to import and override the plugin's settings, however, it didn't stop there. Due to the fact that the plugin used the unserialize function on the user-supplied contents of the `config` parameter for the import, an attacker could craft a special payload that could call other PHP classes and potentially perform other actions if a vulnerable magic method was present in another piece of software installed on the same site. This is referred to as PHP Object Injection, and we have detailed this type of vulnerability more extensively in the post



```php
    if ( isset( $_POST['config'] ) && strlen( trim( $_POST['config'] ) ) > 0 ) {
        $config = maybe_unserialize( base64_decode( trim( $_POST['config'] ) ) );
        if ( is_array( $config ) && count( $config ) > 0 ) {
            update_option( 'heateor_sss', $config );
            header( 'Content-Type: application/json' );
            die( json_encode(
                array(
                    'success' => 1
                )
            ) );
        }
    }
    die;
```

If another plugin or theme with a vulnerable magic method was installed on the same site with a vulnerable version of the Sassy Social Share plugin, then an attacker could potentially have the ability to create new files, delete existing files, execute remote commands, and more. This would make it possible for an attacker to take over a vulnerable WordPress site.

Disclosure Timeline

August 31, 2021 – Conclusion of the plugin analysis that led to the discovery of a vulnerability in the Sassy Social Share WordPress plugin. We develop a firewall rule to protect Wordfence customers, however, after discovering another custom rule provided sufficient protection, we archived the rule.
September 1, 2021 – The vendor confirms the inbox for handling the discussion.
September 2, 2021 – We send over full disclosure details. The vendor responds confirming they will begin working on a fix.
September 2-17, 2021 – We work closely with the vendor to ensure an optimal security patch is released by verifying the implemented fixes before they are released to customers.
September 17, 2021 – The patched version is released as 3.3.24.

Conclusion

In today's post, we described a flaw in the Sassy Social Share WordPress plugin that grants attackers the ability to update the plugin's settings and inject PHP Objects. This flaw has been fully patched in version 3.3.24 of Sassy Social Share. We recommend that WordPress users immediately update to the latest version available, which is version 3.3.25 at the time of this publication.

Please do let others in the WordPress community know about this issue to help them stay safe.

Both Wordfence Premium users and those sites still using the free version of Wordfence have been protected against this any exploits targeting this vulnerability since the vulnerability was introduced in version 3.3.23.

If your site has been compromised as a result of this or any other vulnerability, we offer Professional Site Cleaning services to help undo the damage. If you know a friend or colleague who is using this plugin on their site, please forward this advisory to them to help keep their sites protected as these vulnerabilities can lead to complete site takeover.
Did you enjoy this post? Share it!

Comments

7 Comments

Bow *
October 20, 2021
9:35 am

Thank you for this! I am using Sassy Social Share Premium v. 1.1.36. Could you confirm the premium version of this plugin was also patched? Thank you and great work, as always.

Mark Maunder *
October 20, 2021
10:11 am

Finding out. Stand by.

Mark Maunder *
October 20, 2021
10:14 am

Chloe is buying a premium version to check now. Will get right back to you.

Chloe Chamberland *
October 20, 2021
10:32 am

Hi Bow, I've just reviewed the Sassy Social Share Premium plugin and determined that this vulnerability is not present in v1.1.36 of the plugin, which indicates that the vulnerability was never present in the plugin or has been patched. Thanks!

Bow *
October 20, 2021
2:11 pm

Thanks so much guys! Much appreciated :)

Chloe Chamberland *
October 20, 2021
2:19 pm

You're welcome!

Mike Bourke *
October 20, 2021
8:43 pm

I love that you went the extra mile to confirm that the premium version is not affected by the problem (for whatever reason). Kudos for that.

happens.

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

SIGN UP

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.*

SIGN UP