CSRF Vulnerability Found in Software License Manager Plugin

Updated on September 14, 2021 - Harald Eilertsen

Versions before 4.5.1 of the Software License Manager plugin for WordPress have an exploitable Cross-Site Request Forgery (CSRF) vulnerability. Any user logged in to a site with the vulnerable extension can, by clicking a link, be tricked to delete an entry in the plugin's registered domain database table. The link can be distributed in an email, or on a website the victim user is likely to visit.

The good news is, there's not much else that can be done by exploiting this weakness. And the attacker needs to know the id of the domain they wish to delete from the database beforehand.

Still, we recommend anybody running version 4.5.0 or earlier of the plugin to upgrade as soon as possible.

Details

- **Plugin Name:** Software License Manager
- **Slug:** software-license-manager
- **Plugin URI:** https://wordpress.org/plugins/software-license-manager/
- **Vendor:** Tips and Tricks HQ
- **Vulnerable versions:** <= 4.5.0
- **Fixed in version:** 4.5.1
- **References:** CVE-2021-24711, CWE-352, CVSS: 7.6, CWSS: 40.7

The vulnerability is caused by the handler for the ajax action `del_reistered_domain` (sic) neither performing nonce checks nor authorization of the user performing the action.

```
51  add_action( 'wp_ajax_del_reistered_domain', 'slm_del_reg_dom' );
52  function slm_del_reg_dom() {
53      global $wpdb;
54      $reg_table = SLM_TBL_LIC_DOMAIN;
55      $id        = sanitize_text_field( $_GET['id'] );
56      $ret       = $wpdb->query( "DELETE FROM $reg_table WHERE id='$id'" );
57      echo ( $ret ) ? 'success' : 'failed';
58      exit( 0 );
59  }
```

We always recommend performing nonce checks on any action, and to authorize the user by checking it's capabilities for all non-public action handlers.

The observant reader may also wonder if there is not a SQL Injection vulnerability here. The `$_GET['id']` parameter is expected to be numeric, but this is never validated. However, as WordPress will escape any quotation marks in the request parameters, and the `sanitize_text_field` function will remove any URL encoded octets, the usage here should be safe from exploitation if not necessarily bug free.

Version 4.5.1 addresses both of these issues.

Recommendations

We encourage any site with versions earlier than 4.5.1 of the Software License Manager plugin for WordPress to update as soon as possible.

We strongly recommend that you have a security plan for your site that includes malicious file scanning and backups. Jetpack Security is one great WordPress security option to ensure your site and visitors are safe.

Timeline

2021-09-01: Vulnerability discovered by the Jetpack Scan Team
2021-09-07: Reported to WPScan, contacted vendor.
2021-09-10: Received and verified fixed version from vendor.

*This entry was posted in **Vulnerabilities** and tagged **csrf**, **plugin security**, **Security**, **WordPress**. Bookmark the **permalink**.*

Harald Eilertsen

Harald is a Certified Systems Security Professional (CISSP) with a wide background from software development and the security industry. He has a Master of Science in analog microelectronics from the Norwegian University of Science and Technology (NTNU), and has worked for companies such as Norman, Tandberg and Cisco before joining the Jetpack Scan team at Automattic.

Security (75)
Small Business (16)
Social Media (13)
Support Stories (3)
Tips & Tricks (85)
Uncategorized (5)
Utilities & Maintenance (4)
Vulnerabilities (18)
Website Design (13)
WordAds (1)
WordCamp (3)

Jetpack

EN

WordPress Plugins

Akismet Anti-spam
Jetpack
Jetpack Boost
Jetpack CRM
Jetpack Protect
Jetpack Search
Jetpack Social
Jetpack VideoPress
VaultPress Backup
WP Super Cache

Partners

Recommended Hosts
For Hosts
For Agencies

Developers

Documentation
Beta Program
Contribute to Jetpack

Legal

Terms of Service
Privacy Policy
GDPR
Privacy Notice for California Users

Help

Knowledge Base
Forums
Security Library
Contact Us
Press

Social

Mobile Apps

GET IT ON Google Play
Download on the App Store

An airline

Work With Us