Ram Gall

March 5, 2020

Multiple Vulnerabilities Patched in RegistrationMagic Plugin

On February 24th, our Threat Intelligence team discovered several critical vulnerabilities in RegistrationMagic, a WordPress plugin installed on over 10,000 sites, *including the vendor's own site*.

These allowed an attacker with subscriber-level permissions to elevate their account's privileges to those of an administrator and to export every form on the site, including all the data that had been submitted to them in the past. Additionally, through a number of unprotected AJAX actions, an attacker with subscriber-level permissions could send arbitrary emails, import a custom vulnerable form, replace an existing form with their uploaded form, and use the vulnerable form to register a new administrative user. Finally, none of the administrative functions used by the plugin included nonce checks, making the plugin vulnerable to cross-site request forgery (CSRF) attacks – it was possible for an attacker to forge requests on behalf of an administrator to update any of the plugin's settings.

We privately disclosed these issues to the plugin's author, who released a patch 2 days after receiving our full report. Wordfence Premium users received a new firewall rule on February 25th to protect against exploits targeting these vulnerabilities. Free Wordfence users will receive this rule on March 26, 2020.

Description: Authenticated Privilege Escalation
Affected Plugin: RegistrationMagic – Custom Registration Forms and User Login
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 4.6.0.3
CVE ID: CVE-2020-9456
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CVSS Score: 9.9(Critical)
Patched Version: 4.6.0.4

The RegistrationMagic plugin allows WordPress users to create customized registration forms, track registration submissions, manage users, analyze stats and assign user roles, as well as accept payments.

While quite powerful, there are a number of functions in the plugin used for administrative purposes that are not protected by capability checks or nonces, all of which are processed using custom forms generated by the plugin. Additionally, the plugin automatically creates and publishes a page upon activation, accessible to subscribers at /rm_submissions. This page is intended to allow users to view their previous form submissions, but it could also be used to render and process forms that were only intended to be accessed by administrators. Sending a request to this page with the 'rm_slug' $_POST parameter set to 'rm_user_edit' and the 'user_id' parameter set to the user's ID (which can typically be obtained from the user's profile page) caused the plugin to generate a form which could be used to change the user's role to administrator. Unfortunately, this form didn't use a capability check or a nonce, so it could be used by a subscriber to update their own role to administrator.

```
223 public function edit($model, RM_User_Services $service, $request, $params)
224 {
225     if (isset($request->req['user_id']))
226     {
227         if ($this->mv_handler->validateForm("rm_edit_user"))
228         {
229             if (isset($request->req['user_password']) && isset($request->req['user_password_conf']))
230             {
231                 if ($request->req['user_password'] && $request->req['user_password_conf'] && $request->req['user_id']
232                     $service->reset_user_password($request->req['user_password'], $request->req['user_password_conf']
233                 $service->set_user_role($request->req['user_id'], $request->req['user_role']);
```

Description: CSRF to Settings Modification
Affected Plugin: RegistrationMagic – Custom Registration Forms and User Login
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 4.6.0.3
CVE ID: CVE-2020-9454
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
CVSS Score: 8.0(High)
Patched Version: 4.6.0.4

Not only did the RegistrationMagic plugin fail to check nonces in the previously mentioned vulnerability, it actually did not check nonces for *any* of its functionality, including the forms used to save changes to the plugin settings. As such it was possible for an attacker to forge a crafted request on behalf of a site administrator in order to modify the plugin's settings, which included the ability to delete existing users or add new user roles. It could even be used to allow forms to accept php files, which could then be used to upload a backdoor which could allow an attacker full control over the WordPress site.

Description: Authenticated Email Injection
Affected Plugin: RegistrationMagic – Custom Registration Forms and User Login
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 4.6.0.3
CVE ID: CVE-2020-9455
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
CVSS Score: 6.4(Medium)
Patched Version: 4.6.0.4

In addition to allowing a subscriber to elevate their privileges, the RegistrationMagic plugin also allowed a subscriber to send emails from the site to any email address, with a subject and body of their choice. This could be used to send spam, but this flaw would also make tricking a site administrator into clicking a link in order to perform a CSRF attack much easier. This functionality actually used an unprotected AJAX action, which is an extremely common attack vector in WordPress. Although it was only available to subscribers, much of the plugin's functionality was geared towards an improved user experience for subscribers, so this was a surprising oversight.

```
$this->loader->add_action('wp_ajax_send_email_user_view', new RM_User_Services(), 'send_email_ajax');
```

```
public static function send_email_ajax()
{
    $to = $_POST['to'];
    $sub = $_POST['sub'];
    $body = $_POST['body'];

    RM_Utilities::quick_email($to, $sub, $body);

    wp_die();
}
```

As you can see, the 'send_email_ajax' function doesn't use any capability or nonce checks, so any logged-in user could use it to send email from the site.

Description: Authenticated Settings and User Data Export
Affected Plugin: RegistrationMagic – Custom Registration Forms and User Login
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 4.6.0.3
CVE ID: CVE-2020-9458
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CVSS Score: 4.3(Medium)
Patched Version: 4.6.0.4

Using the same /rm_submissions endpoint as the authenticated privilege escalation vulnerability, a logged-in attacker could also send a request with the 'rm_slug' $_POST parameter set to 'rm_form_export', which caused the plugin to export every form on the site, *including everything that had ever been submitted to any of these forms* (though this did not include login credentials). Again, the export function lacked access control or a nonce check, and in addition to exposing potentially sensitive information, an attacker could use the exported form data to launch yet another type of attack. For those sites with sensitive personally identifiable user information, such as commerce sites, this vulnerability was particularly concerning.

*The vulnerable function has more than 230 lines of code. For brevity, we're not showing it here, but it is available to review in the plugin repository.

Description: Authenticated Settings Import -> Privilege Escalation
Affected Plugin: RegistrationMagic – Custom Registration Forms and User Login
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 4.6.0.3
CVE ID: CVE-2020-9457
CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H
CVSS Score: 8.0(High)
Patched Version: 4.6.0.4

There was one more method an attacker could use to create an administrator, though it took a bit more work and a few more steps. One of the more advanced features of the RegistrationMagic plugin allowed the creation of forms that saved user-submitted content directly into the usermeta table in the site's database. While this functionality was intended to store additional metadata about the user, this table is *also* used to store a user's permissions, using the wp_user_level and wp_capabilities keys, and a custom form could be created to modify the contents of these keys. Another advanced feature was the ability to make forms "expire" after a certain date or number of submissions, and to automatically substitute a different form at that time.

Unfortunately, thanks to more unprotected AJAX actions, an attacker could upload a customized "vulnerable" registration form. They could then use the data export vulnerability to grab the information they needed to launch the next step: by using yet another unprotected AJAX action, they could set an existing form on the site to expire after 0 submissions, and replace it with their newly uploaded form. Once the vulnerable form was active, the attacker could register as an administrator.

If no forms were published, but the plugin's "Magic Button" functionality was enabled, an attacker could also use an unprotected AJAX action to set their uploaded form as the "Default" form, which could be submitted from anywhere on the site.

The registered AJAX actions:

```
$this->loader->add_action('wp_ajax_rm_save_form_view_sett', new RM_Form_Settings_Controller(), 'view');
```

```
$this->loader->add_action('wp_ajax_set_default_form', 'RM_Utilities', 'set_default_form');
```

```
$this->loader->add_action('wp_ajax_import_first', 'RM_Services', 'import_form_first_ajax');
```

```
$this->loader->add_action('wp_ajax_rm_admin_upload_template', $rm_admin, 'upload_template');
```

The vulnerable functions – note the lack of capability checks and nonce checks:

```
public function upload_template(){
    if($_FILES){
            $name=get_temp_dir().'RMagic.xml';
            if(is_array($_FILES['file']['tmp_name']))
            $status= move_uploaded_file ( $_FILES['file']['tmp_name']['0'] , $name );
            else
            $status= move_uploaded_file ( $_FILES['file']['tmp_name'], $name );
            echo json_encode(array('success'=>$status));
    }
```

```
public static function import_form_first_ajax() {
    $form_id = null;
    if (isset($_POST['form_id'])) {
        $form_id = $_POST['form_id'];
    }
    echo self::import_form_first(null, $form_id);
    wp_die();
}
```

```
function view($model=null, $service=null, $request=null, $params=null) {
    if (!$request instanceof RM_Request) {
        $postdata = file_get_contents("php://input");
        $request = json_decode($postdata);
        if(isset($request->form_id) && (int)$request->form_id){
            $model = new RM_Forms;
            $model->load_from_db($request->form_id);
            $model->set((array)$request);
            $model->update_into_db();
            echo 'saved';
```

```
1180 | public static function set_default_form() {
1181 |     if (isset($_POST['rm_def_form_id'])) {
     |
1186 | }
```

Disclosure Timeline

February 21, 2020 – Lower-severity vulnerabilities discovered with indications that higher-severity vulnerabilities might be present.
February 24, 2020 – Higher-Severity vulnerabilities discovered and analyzed.
February 25, 2020 – Firewall rule released for Wordfence Premium users. Initial outreach to plugin vendor.
February 26, 2020 – Vendor confirms appropriate inbox for handling discussion. Full disclosure of vulnerabilities is sent.
February 28, 2020 – Vendor releases an update patching vulnerabilities.
March 26th, 2020 – Firewall rule becomes available to free users.

Conclusion

In today's post, we detailed several vulnerabilities including CSRF, email injection, and privilege escalation found in the RegistrationMagic plugin. These flaws have been patched in version 4.6.0.4, and we recommend that users update to the latest version available immediately. While we have not detected any malicious activity targeting RegistrationMagic, some of these vulnerabilities are severe enough to allow complete site takeover. Sites running Wordfence Premium have been protected from attacks against this vulnerability since February 25th. Sites running the free version of Wordfence will receive the same firewall rule update on March 26th, 2020.

Did you enjoy this post? Share it!

Comments

3 Comments

Syxguns *
March 5, 2020
3:23 pm

Wow, I use RegistrationMagic Premium and I've had the latest update for well over a week. I just went to https://metagauss.com/ who is the site that holds the plugins for RegistrationMagic and ProfileGrid. The version to download is still v4.6.0.1.

RegistrationMagic.com is down or responding very slow and the pages do not display properly. However, ProfileGrid.co comes up as well as metagauss.com. You have me a little worried about reading this post. I'll check again tomorrow to se if a newer version is available.

Ram Gall *
March 13, 2020
11:33 am

Hi Syxguns!

It looks like the plugin vendor has updated RegistrationMagic Premium at this time, and it now contains security fixes to address these vulnerabilities.

Kad *
March 6, 2020
1:41 am

No nonce checking, no capability/privilege checking... Where have I seen this before...

Breaking WordPress Security Research in your inbox as it happens.

you@example.com

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

© 2012-2022 Defiant Inc. All Rights Reserved