Chloe Chamberland

September 22, 2021

Recently Patched Vulnerabilities in Ninja Forms Plugin Affect Over 1 Million Site Owners

On August 3, 2021 the Wordfence Threat Intelligence team initiated the responsible disclosure process for two vulnerabilities that were discovered in Ninja Forms, a WordPress plugin installed on over 1,000,000 sites. These flaws made it possible for an attacker to export sensitive information and send arbitrary emails from a vulnerable site that could be used to phish unsuspecting users.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on August 2, 2021. Sites still using the free version of Wordfence received the same protection on September 1, 2021.

We sent the full disclosure details to Ninja Forms on August 3, 2021, as per the security disclosure policy listed on Ninja Forms website. Ninja Forms quickly acknowledged the report the same day and informed us that they would start working on a patch immediately. A patch was released on September 7, 2021 in version 3.5.8.

We strongly recommend updating immediately to the latest patched version of Ninja Forms to patch these security issues, which is version 3.5.8.2 of Ninja Forms at the time of this publication.

Description: Unprotected REST-API to Sensitive Information Disclosure
Affected Plugin: Ninja Forms
Plugin Slug: ninja-forms
Affected Versions: <= 3.5.7
CVE ID: CVE-2021-34647
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.5.8

Ninja Forms is one of the most popular form building plugins for WordPress websites. One feature the plugin offers is the ability to export all of a site's form submissions for reviewing and analyzing submission data. Unfortunately, this was insecurely implemented making it possible for any authenticated user to export all of a site's submission data.

The plugin registered a rest route `/ninja-forms-submissions/export` which did in fact use a `permissions_callback`. However, this check did nothing more than validate whether or not a user was logged in through the `is_user_logged_in()` function. There was no check to verify if a user had the appropriate permissions to execute the function.

```
83  public function permission_callback(WP_REST_Request $request) {
84
85      //Set default to false
86      $allowed = false;
87
88      //Check Capability of logged in users
89      $allowed = is_user_logged_in();
```

This meant that any logged-in user could use the `/ninja-forms-submissions/export` endpoint and export everything that had ever been submitted to one of the site's forms. Depending on how a site's forms were configured this data could contain sensitive personally identifiable information (PII) that would provide an attacker with valuable information to conduct other attacks.

Description: Unprotected REST-API to Email Injection
Affected Plugin: Ninja Forms
Plugin Slug: ninja-forms
Affected Versions: <= 3.5.7
CVE ID: CVE-2021-34648
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.5.8

In addition to the previous bulk submission export vulnerability, there was another functionality in the plugin that was insecurely implemented using the same vulnerable `permissions_callback` validation.

The plugin registered the `/ninja-forms-submissions/email-action` endpoint which was intended to trigger bulk email actions on form submissions. This functionality was intended to allow site owners to trigger a variety of email actions like sending an email confirmation, or email notification, in bulk in response to user submissions.

Unfortunately, due to the fact that this functionality used the same `permissions_callback` check, any authenticated user could trigger an email action using the REST-API endpoint. To make matters worse, the `trigger_email_action` function executed by the `email-action` endpoint crafted the email based on values that could be passed in the request. This made it possible for an attacker to craft a completely unique email, which included the body and subject, and then send it from the vulnerable site to any email address.

```
public function trigger_email_action(WP_REST_Request $request) {
    //Extract required data
```

```

    //Throw error if we're missing data
    if( !isset($data) || empty($form) || empty($sub) ) {
        return new WP_Error( 'malformed_request', __('This request is missing data', 'ninja-forms') );
    }

    //Process Merge tags
    $action_settings = $this->process_merge_tags( $data->action_settings, $data->formID, $sub );
    //Process Email Action
    $email_action = new NF_Actions_Email();
    $result = $email_action->process( (array) $action_settings, $data->formID, (array) $field_values );

    //Return true if wp_mail returned true or the submission ID if it failed.
    $return = !empty($result['actions']['email']['sent']) && true === $result['actions']['email']['sent'] ? $result[

    return $return;
```

This vulnerability could easily be used to create a phishing campaign that could trick unsuspecting users into performing unwanted actions by abusing the trust in the domain that was used to send the email. In addition, a more targeted spear phishing attack could be used to fool a site owner into believing that an email was coming from their own site. This could be used to trick an administrator into entering their password on a fake login page, or allow an attacker to take advantage of a second vulnerability requiring social engineering, such as Cross-Site Request Forgery or Cross-Site Scripting, which could be used for site takeover.

Disclosure Timeline

August 2, 2021 – Conclusion of the plugin analysis that led to the discovery of two vulnerabilities in the Ninja Forms WordPress plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users.
August 3, 2021 – We send over full disclosure details. The vendor confirms they have received the details and will begin working on a fix.
August 31, 2021 – We follow-up with the vendor to check on the status of the security fixes.
September 1, 2021 – Wordfence free users receive the firewall rule. We receive an update that the security fixes are in place and ready to be released. The vendor informs us that they will follow-up with an estimated release date.
September 6, 2021 – We receive an update that the patched version will be released in a few days.
September 7, 2021 – A newly updated version of the plugin, 3.5.8, is released containing sufficient patches.

Conclusion

In today's post, we detailed two flaws in Ninja Forms that granted attackers the ability to export sensitive data and send arbitrary emails from any vulnerable site. These flaws have been fully patched in version 3.5.8. We recommend that WordPress users immediately update to the latest version available, which is version 3.5.8.2 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on August 2, 2021. Sites still using the free version of Wordfence received the same protection on September 1, 2021.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as these are serious vulnerabilities that can lead to sensitive information disclosure.

Click here to join the WordPress Security mailing list and receive vulnerability reports like this the moment they are published.
Did you enjoy this post? Share it!

Comments

No Comments