N5 Upload Form <= 1.0 - Unauthenticated Arbitrary File Upload

An arbitrary file upload vulnerability in N5 Upload Form in current version 1.0 allows the remote attackers to upload arbitrary executable files and achieve the remote code execution. The plugin provides a file uploading form to the plugin user and allows the user to decide which directory is used for the uploading files in the local operating system. But it does not ensure that the directory cannot be accessed by the remote attacker, and the extension of the file is also unrestricted.

Proof of Video

In order to provide the file uploading functionality, It uses move_uploaded_file() function to store the file to the directory that decided by the plugin user. However, it only checks whether the directory is existing or not and failed to check file extension before use the move_uploaded_file() function.

```
<?php
if ($post_meta['usernotice'] == 0 && !file_exists($post_meta['directory'])) {
    $upload_errors[] = __('The uploading failed.', 'N5_UPLOADFORM');
}

if (count($upload_errors) == 0) {
    $file['uploadedname'] = sprintf("%s.%s", md5(uniqid(rand())), $file['ext']);
    move_uploaded_file($file['obj']['tmp_name'], sprintf("%s/%s", $post_meta['directory'], $file['uploadedname']));
}
...
```