

# [VulnWatch] Coppermine Photo Gallery remote compromise

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0014.html>

---

**From:** Berend-Jan Wever ([SkyLined@edup.tudelft.nl](mailto:SkyLined@edup.tudelft.nl))

**Date:** 04/07/03

From: "Berend-Jan Wever" <[SkyLined@edup.tudelft.nl](mailto:SkyLined@edup.tudelft.nl)>

To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>, <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>, "Windows NTBugtraq Mailing L

Date: Mon, 7 Apr 2003 18:47:57 +0200

---AFFECTED SOFTWARE---

From the website, <http://www.chezgreg.net/coppermine/>:

"Coppermine Photo Gallery is a picture gallery script. Users can upload pictures with a web browser (thumbnails are created on the fly), add comments, send e-cards and view statistics about the pictures. "

"The script use PHP, a MySQL database and the GD library (version 1.x or 2.x) or ImageMagick to make the thumbnails. An install script makes the installation very fast and easy."

The problem was found in Coppermine 1.0 RC3, the latest stable release. The latest beta (1.1 beta 2) is not affected according to the author.

---PROMBLEMS---

Coppermine allows the uploading of images onto a server by logged in users and in a lot of configurations even anonymous uploading. The upload script has a buggy extention checking routine which allows the uploading of ".jpg.php" files. These files need to be a valid jpg-files or Coppermine will delete them. It is trivial to create a file which is a valid jpg and also a valid PHP script. Once uploaded, the PHP script can then be executed, allowing access to the remote server under the priviledges of the user PHP is running under.

---EXPLOIT---

Attached is a working exploit, upload this onto a vulnerable server and execute it like this:

`/albums/userpics/Copperminer.jpg.php?[command]`

Where command can be something like "id;uname%20-a" or "cat%20/etc/passwd"

Note 1: MSIE will display Copperminer.jpg.php as an image, but lynx will display the output of the command you gave it.

Note 2: <http://www.google.com/search?q=allinurl%3A+/upload.php?album=>

## VulnWatch: [VulnWatch] Coppermine Photo Gallery remote compromise

### ---TIMELINE---

mar 31, 2003 – Issue discovered, working exploit written.  
mar 31, 2003 – Author contacted, problem acknowledged by author.  
apr 05, 2003 – Patches released through Coppermine website.  
apr 07, 2003 – Information disclosed.

### ---PATCH---

Can be found at <http://www.chezgreg.net/coppermine/>

Kind regards,

Berend-Jan Wever

<http://spoor12.edup.tudelft.nl>

- 
- application/octet-stream attachment: [Copperminer.jpg.php](#)