

29 September 2008

By: Lucian Constantin, Web News Editor



ImageShack URL manipulation discloses uploaders' IPs
ImageShack for the logo

[ImageShack Flaw Exposes the IP Addresses of Uploaders](#)

A security issue allows access to upload information files associated with images

[Christopher Boyd](#), Director of Malware Research for FaceTime Security Labs and Microsoft Security MVP, has come across a security flaw on the popular free image hosting service ImageShack through which anyone could have downloaded the log file associated with any image. Such a log file contains the IP address which was used to upload a particular image.

The file/directory permission related vulnerability was easily exploitable through URL manipulation, a user only needing to change the file extension from .jpg to something else in an ImageShack direct URL. Not being able to parse the Content-Type the browser offered this new file for download. Upon opening it in any text editor, the IP address of the uploader would have been revealed.

Being able to see the IP of anyone who uploaded an image on the website poses a very serious privacy issue. "Considering they have 2+ million uploads a day, that's an awful lot of people to choose from," notes Christopher Boyd. He also gives several examples of what one might do with this piece of information. They range from scaring people on forums by revealing their IP to running exploits against their computers.

He also mentions the possibility of ratting out on employees for uploading files to ImageShack while at work, using such websites from company offices being usually prohibited. "It may sound a touch OTT, but never underestimate someone's capacity to cause trouble over the silliest things," says Mr. Boyd on his blog.

ImageShack has acted promptly and addressed the issue in less than one hour. The ImageShack reply expressed their confidence that "this security gap no longer exists". This looks to be the case as trying to exploit it now will return a 403 - Forbidden error, which most likely means that directory/file permissions on the Web server have been corrected. "I can't remember the last time we found something that was patched at such speed, and full credit to them," notes Boyd.

Apparently, a very similar information disclosure incident occurred on the ImageShack website back in 2006. A permission issue allowed users to download the entire post logs for each of the 520 different ImageShack servers by accessing a URL of the type `http://img##.imageshack.us/logs/postlog` (where ## represent digits forming the server number). The logs contained names of the uploaded images, their respective uploader's IP, date of upload and the upload hash, which could have been used to search the log for all images uploaded by the same person.