

# SECURITY ADVISORY

**November 2007**

punBB imgUpload extension



## **Table of Contents**

The Security Research Team.....	2
Brief Issue Description .....	3
Affected Components .....	3
Finding Affected Sites with This Issue .....	3
Issue History .....	3
Example Attack: Compromising the Web Server.....	4
Example Attack: Attacking Clients Through Cross-Site Scripting .....	4
Issue Mitigation .....	5
CVSS Issue Severity Scores .....	5

## **About FortConsult**

FortConsult is an unbiased, vendor independent security consulting company, based in Copenhagen, Denmark, and operating throughout Europe.

We are experts in discovering and managing vulnerabilities in applications and in IT infrastructure such as network equipment and servers.

We are also certified by VISA and MasterCard to perform PCI Data Security Standard audits.

If you would like to hear more about our services, or need assistance in solving a specific security problem, please visit [www.fortconsult.net](http://www.fortconsult.net) or call +45 7020 7525.

## **Copyright and Disclaimer**

The information in this advisory is Copyright 2007 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

## **The Security Research Team**

This advisory has been discovered by FortConsult's Security Research Team (team-member: Peter Österberg), as part of a general investigation into the security of software used in common IT environments.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information see [www.fortconsult.net](http://www.fortconsult.net).

The SRT can be contacted at: [teknik@fortconsult.net](mailto:teknik@fortconsult.net); Peter can be contacted at [poe@fortconsult.net](mailto:poe@fortconsult.net).

### ***Brief Issue Description***

This advisory affects a vulnerability found in an image upload add-on to the popular forum software punBB, the add-on is called imgUpload. It is used for allowing the users of punBB to upload pictures to their postings.

The add-on does by default allow images in the file formats .jpg, .gif and .png to be uploaded to the server. The file is simply uploaded and a thumbnail picture is created along with it. The user will be given a link to the picture which is supposed to be copied, as a link to the picture, into the forum posting.

The add-on does however only check the mime type given by the web browser, to if the file is of a valid file type. Any file with any extension can be uploaded as long as the mime type is set to any of the three allowed image formats.

The thumbnail generation will fail but the original file will still be correctly uploaded and the generated URL that imgUpload wants the user to copy into the forum will link to the uploaded file that contains arbitrary content.

This opens up the possibility to upload files with persistent cross site scripting content and it does furthermore also allow uploading of PHP files that can be executed on the server platform.

The generated link that the user has to post into the forum will contain the uploaded file's original extension.

### ***Affected Components***

punBB version 1.2.14

Automatic Image Upload with thumbnails – uploading.php - add-on version 1.3.2

### ***Finding Affected Sites with This Issue***

Normal Google hacking techniques can be used to discover site's with the vulnerable PHP program.

### ***Issue History***

Nov 28 2007	FortConsult discovered the vulnerability
Nov 29 2007	Vendor informed by FortConsult
Jan 01 2008	Tentative public disclosure date

### ***Example Attack: Compromising the Web Server***

1. Create a file in a text editor with arbitrary executable content (PHP is the obvious choice).
2. Upload the file to the server, using a pen-tester's web proxy like Paros.
3. Alter the MIME type to image/jpeg in the proxy.
4. Note the URL returned by the web server – this is where the executable file has been uploaded to.
5. Browse the returned URL; the code will be executed.

### ***Example Attack: Attacking Clients Through Cross-Site Scripting***

6. Create a file in a text editor with arbitrary html content, including the <html> and <body> tags.
7. Save the file as <name>.jpg
8. Upload the "image" using the image upload link inside the punBB forum, this link can be found at the bottom of the posting window when writing a new forum posting
9. Paste the link given into the posting window and save the posting
10. View the newly saved post and click the link

The browser, if vulnerable, will now show the parsed html of the file uploaded.

## ***Issue Mitigation***

Non known at this time, consider turning off the image upload functionality while awaiting a vendor patch.

To prevent the most severe issue, PHP code upload, configure the webserver so that uploaded "image" files are placed in a directory which is configured to prevent execution.

## ***CVSS Issue Severity Scores***

The issues described in this advisory have received a base score of 10 (the most severe score possible). The score is based on the following criteria.

FortConsult has used the online CVSS calculator found at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

### **BASE METRICS: 10**

Access Vector:	Remote
Access Complexity:	Low
Authentication:	Not Required
Confidentiality Impact:	Complete
Integrity Impact:	Complete
Availability Impact:	Complete
Impact Bias:	Confidentiality

**FORTCONSULT**

*Straight talk on IT security*