

# [NT] PHP for Windows Arbitrary Files Execution (GIF, MP3)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0106.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 02/17/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 17 Feb 2002 15:42:50 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

PHP for Windows Arbitrary Files Execution (GIF, MP3)

---

## SUMMARY

Through PHP.EXE, an attacker can cause PHP to interpret any file as a PHP file, even if its extensions are not PHP. This would enable the remote attacker to execute arbitrary commands, leading to a system compromise.

## DETAILS

Vulnerable systems:

PHP version 4.1.1 under Windows

PHP version 4.0.4 under Windows

An attacker can upload innocent looking files (with mp3, txt or gif extensions) through any uploading systems such as WebExplorer (or any other PHP program that has uploading capabilities), and then request PHP to execute it.

Example:

After uploading a file a "gif" extension (in our example huh.gif) that contains PHP code such as:

Securiteam: [NT] PHP for Windows Arbitrary Files Execution (GIF, MP3)

```
#-----  
<?  
phpinfo();  
>  
#-----
```

An attacker can type the following address to get in to cause the PHP file to be executed:

[http://www.example.com/php/php.exe/UPLOAD\\_DIRECTORY/huh.gif](http://www.example.com/php/php.exe/UPLOAD_DIRECTORY/huh.gif)

Notice: php/php.exe is included in the URL.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:compume2000@hotmail.com>> CompuMe and <<mailto:condor@phreaker.net>> RootExtractor.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Website Pro Path Disclosure (%20, ")"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)