

Joomla 1.5.x Viagra Hack Information and Fix

Posted on Mar 27, Posted by [Jacob Hodara](#) Category [Security](#)

In the past week alone we've had two clients reach us about their site being hacked.

The hack injected numerous "Buy Viagra" links into their websites right below the `<!--` tag. The hack only displays for User Agent Googlebot, that means if you are using Firefox or Internet Explorer you will not see these links when viewing the source code, only Chrome.

Upon further investigation, comparing site and original Joomla 1.5.x source code we've located the file to be located in:

`/libraries/joomla/application/application.php`

If your file is over 30KB in size, you are infected. Another way to find out if you are infected is to search Google for your website name as well the word Viagra, if you find results, you are infected.

January 2013 Update

I have seen more cases of `/libraries/joomla/session/session.php` being hacked as well with an include file from the tmp directory.

Your next action:

Upgrade to Joomla 2.5/3.x immediately.

Short term solution:

- Change your admin + FTP passwords
- Upgrade all 3rd party modules/plugins/components
- Upgrade to latest Joomla 1.5.x series
- Lock down FTP to your IP address

Hire an affordable Joomla expert

For your **free, no obligation estimate** please [contact us today](#) .

Tags: [hack](#) , [joomla](#) , [security](#)