Site hacked due to Single Sign-In plugin?

Posted by jimmywiddle - 2016/01/15 09:45

Hi, Im currently using the latest Joomla version 3.4.8 and your Single Sign-In for domains plugin V1.0.11 downloaded only a 3 months ago.

It seems that my site has been hacked and I have found 2 files in the root that shouldn't be there and also my whole site and admin was white screen (with the debug errors below) until I renamed the /multisites_ssidomains/ directory.

Please can you get back to me asap on this, my host is also suggesting your plugin is to blame :(

Warning: require_once(/plugins/system/multisites_ssidomains/multisites_ssidomains.php) : failed to open stream: Permission denied in /libraries/cms/plugin/helper.php on line 230

Fatal error: require_once() : Failed opening required '/plugins/system/multisites_ssidomains/multisites_ssidomains.php' (include_path='.:/opt/alt/php53/usr/share/pear:/opt/alt/php53/usr/share/php') in /libraries/cms/plugin/helper.php on line 230
==========

==========

Re: Site hacked due to Single Sign-In plugin?

Posted by edwin2win - 2016/01/15 10:21

First, I can tell you that your affirmation to have been hacked using the SSI for domain is not possible.
There is no upload files and save of files inside the SSI for domains.

For your information, we have reported to Joomla JSST the 30-dec-2015 a new security vulnerability that affect J3.4.8 and we can tell you that other vulneratbilities exists in this Joomla version.

When a hacker arrives to enter, in general they update plenty of files and also add back-doors that they can re-exploit later when you fix a hack.
So retore a website that has been hacked is not necessarly easy.
You have to check if you have a good an clean backup for a restore.

Most of the exploit that we have identified tried using a vulnerability inside the joomla "content history" (including in J3.4.8).
We recommend that you disable this extension from the extension manager.
This is will reduce your risk under J3.4.8

What may happen is that the hacker modified one of our sources in the SSI for domain to add a back-door.

Becarefull, don't trust the date of the files to identify which one where hacked.
The hacker in general restore the date to avoid show that a file is hacked.

A possiblity to identify all the hacked files is to compare your current "hacked" website with a clean backup.

You will probably discover plenty of files added and files updated.

Remark: The latest J3.4.6 and higher fixes was due to a combinaison of the PHP version, Browser user agent and session management.
They was frequently also exploited via the "content history" extension.

I hope this will help you restoring you environment and also identifying the way that the hacker is entered.

==========

Re: Site hacked due to Single Sign-In plugin?

Posted by jimmywiddle - 2016/05/30 14:11

Hi, Since restoring from a clean backup etc etc etc everything has been fine for months now.

But ive just noticed the single-sign in is not working now, the user is logged into the site logged into and not the other, ive checked everything and got nowhere, your help would be very much appreciated!

Im aware your need a link to the site, by im reluctant to post it here, Ive sent you an email also though, with the link.

Hoping to hear from you soon!
Many thanks in advance!

==========