3082/13

GOVERNMENT OF KERALA

INFORMATION TECHNOLOGY (B) DEPARTMENT

No. 639/B2/13/ITD **Dated: 20/03/13, Thiruvananthapuram.**

CIRCULAR

Sub:- IT Department- Security Audit of Government of Kerala Websites hosted at SDC- Prevention of Security breaches to official websites. Security measures to be adopted- Instructions issued-reg.

Computer Emergency Response Team-Kerala (CERT-K) under Kerala State IT Mission (KSITM) recently conducted a Security Auditing of all Government of Kerala Websites currently hosted at State Data Centre(SDC) with an objective to identify the vulnerabilities and to suggest recommendations for fixing the same. The Security Audit Report reveals that there are several vulnerabilities present in Websites which require immediate attention. It is also revealed that majority of the websites hosted in SDC do not follow any basic security policies of the Centre Management Frame Work(CMF) which means that these websites are running under high risk. No maintenance or updation are taking place in the installed components/modules in many websites, which may lead to severe security issues.

Under this circumstances all Heads of Departments are hereby instructed as follows:

1. SDC guidelines regarding security auditing of websites should be strictly followed while hosting websites.
2. All web applications shall be STQC verified and the cost of STQC verifications should be included in the project proposal stage itself(so that complaints of lack of funds for STQC certifications are not received after the website is developed completely).
3. There are several defacement of websites happening due to old Joomla CMF usage. It should be avoided and suitable software patches of new Joomla CMF be installed.

4. CERT-K will be doing periodic audit of security vulnerabilities and these will be intimated to the concerned agencies/departments. They shall address these concerns and take corrective action by 3 months. Otherwise the websites will be brought down from SDC.

5. All subsequent modifications done after the website is rolled out in the SDC should also be STQC verified.

6. Proper security updates should be done to the sites and modules and to ensure that all sites should go through security auditing checks by authorised agencies.

Measures to strengthen the security of the official websites may be done within a week time as per the Recommendations and Counter Measures annexed to this circular. The detailed Website Audit Report of departments will be provided by CERT-K, KSITM on request.

P.H. Kurian
Principal Secretary to Government.

To
All Heads of Departments.
Director, I&PRD.
Director, CERT-K, Thiruvananthapuram.
Director, Kerala State IT Mission, Thiruvananthapuram.
Stock File/Office Copy.

Forwarded / By Order

Section Officer

Allow from all

</FilesMatch>

The above code means that only files that have a jpeg or a pdf extension are allowed to be uploaded to the website.

4. Always keep your Joomla website up-to-date with the latest version of Joomla:

Every Joomla update addresses security issues that are known to the Joomla community at the time of the update. If you leave your website without updates for a long time, then it will be almost a certainty that your website will be hacked.

5. Upgrade all third party scripts to latest version:

Make a list of all the scripts you use. For each, if you are not using the latest version, upgrade now. To find latest version information for some common scripts, and to view the latest security advisories please refer Secunia.com. The Secunia page often lists vulnerabilities found in plug-ins or add-ons. Check these, too. If there is a recent security advisory for a script you use that is outdated, there is a good chance you've found the reason your site was hacked.

Refer the following URLS for more information

http://secunia.com/advisories/search/?search=Joomla

http://docs.joomla.org/Vulnerable_Extensions_List

http://secunia.com/advisories/product/5788/?task=advisories

6. Hide your Joomla version:

Telling the world about your Joomla version in your HTML code is like inviting malicious attacks to your own doorstep.

7. Change the Default Database Prefix (jos_)

While installation, change the default database prefix to something

Annexure

CERT-K

Recommendations and Counter Measures

1. **Strengthen the web server security:** It is very essential to follow and use best security practices for designing, implementing the public access web servers before deployment. Government of India published necessary guidelines for securing web server. Kindly refer the following guidelines for web server security.

   www.cert-in.org.in/Downloader?pageid=6&type=2&filename=CISG-2004-04.pdf

   www.cert-in.org.in/Downloader?pageid=6&type=2&filename=CISG-2008-01.pdf

2. **Prevent Web Server from execution of PHP Shells**

   Please note that the PHP shell is one type of hacker's control panel on web servers monitor by hackers. php.ini is a configuration file that is used to customize the behaviour of PHP at run time. php.ini file contains settings for upload directory, register global variables, display errors, log errors, max uploading size setting, maximum time to execute a script and other configurations. Server can prevent the execution of PHP shells by adding few codes like *php_uname, getmyuid, shell_exec,escapeshellarg, escapeshellcmd* in the 'php.ini' configuration file.

3. **Restricting uploads using .htaccess**

   The .htaccess file is used for securing the files and directories on the server where the website is hosted. .htaccess can override any particular server's global configuration, placing files within the web tree and configuring a particular directory and all of its subdirectories. For restricting uploads to the website, we can use .htaccess whitelist.

   An .htaccess whitelist consists of specifying which file types can be uploaded to the website in the .htaccess file. It can be done by adding the following code to the .htaccess file:

   ```
   <FilesMatch "\.(jpeg|pdf)$">
   ```

can use to protect your Joomla! website from intrusions and hacker attacks.

- **jSecure** :- jSecure Authentication module prevents access to administration (back end) login page without appropriate access key.

Block Direct access to Administrator page of website:-

Attackers can easily determine that your site runs Joomla! by appending "/administrator" to your domain name (http://your-domain.com/administrator) and also he can run automated scripts to break your credentials. It can be prevented easily by appending the below lines allows an administrator to add an access key to the end of the URL which will redirect wrong entries to the homepage without ever seeing the administrator login panel.

Blocking the direct access to the Joomla administrator page

Step 1 : Go to the administrator directory of your Joomla website.

Step 2 : Open the index.php, copy and paste the below line .

```
/* Block direct access to administrator
-------------------------------------------------- */
$user =& JFactory::getUser();
$secretkey = 'abcd';
$redirectto = 'location: ../index.php';
$usertype = 'Registered';
//Check if the user is not logged in or if is not a super user:
if ($user->guest ) {
//Check if the secret key is present on the url:
if(@$_GET['access'] != $secretkey) { header($redirectto); }
}
```

random. This will prevent most of the SQL injection attacks as hackers try to retrieve super admin details from jos_users table.

8. Change super administrator username

Change the username for the super-administrator. By default, its admin. So change it something like azx.david so that the username/password combination becomes difficult to guess or crack.

The default ID for the admin user in Joomla is always 62, and this may be used by a hacker. To avoid this, do the following:

- Create a new super-administrator with another user name and a strong password
- Log out and in again as this new user
- Change the original admin user to a manager and save (you are not allowed to delete a super-administrator).
- Now, delete the original admin user (user ID 62).

9. Strong password

Always use strong password for the administrator accounts. An example of strong password is E@ M!$ 2@k (min of 10 characters).

A good addition is to password protect the administrator folder. In apache web server, you can do this .htaccess file or in cpanel, you can use Password Protected Directory option to setup a password. This will add another layer of username/password before someone reaches your Joomla admin details. Needless to say, have this password different from Joomla admin password

10. Change your username and password often

At least every 3 months, changing your password regularly is a very healthy practice for your website's security.

11. Use Security extensions like

- **RSFirewall** :-It is the most advanced Joomla! security service that you

hacking attempts occur due to vulnerability in these extensions. Download Joomla/extensions from official sites only such as Joomlacode.org and check the MDH hash. So, always use extensions which are popular, has strong community backing and development process.

- Check how many people downloaded/reviewed the extension.If the number is small, then avoid the extension altogether.
- Check the reviews by the people who have installed the extension. Are there reviews complaining about security issues with this particular extension? If you even find one such review, then avoid the extension altogether.

15. Use Proper Antivirus for your machine

Malware, Spyware and other computer infections once accounted for the vast majority of website hacks, people's awareness of viruses and better quality antivirus have reduced this form of hacking. Run regular full system checks against all machines that are used to access/update your website, be careful / vigilant when browsing the Internet and opening emails. Don't risk your businesses reputation, keep your computers clean and free from infections.

/* ---------- */

Just above echo JResponse::toString($mainframe->getCfg('gzip'));

Step 3: For accessing your website administrator page

Examples :

Without the key --> redirects to the homepage:

http://yourdomain.com/administrator

With the key --> allows you to access the login page

http://yourdomain.com/administrator?access=abcd

Note : The secret key = "abcd" can be modified according to you.

12. Delete leftover files

When you installed an extension that you didn't like, don't set the extension to unpublished. If you do, the vulnerable files will still be on your website. So simply use the un-install function to totally get rid of the extension.

13. Use the correct CHMOD for each folder and file

Setting files or folders to a CHMOD of 777 or 707 is only necessary when a script needs to write to that file or directory. All other files should have the following configuration:

- PHP files: 644
- Config files: 666
- Other folders: 755

14. Only install reliable and community-trusted extensions:

There are more than 4000 extensions available for Joomla many of which are non-commercial. But don't take this as an opportunity to install unnecessary extensions on your website. Remember that most