I/6109747/2024

GOVERNMENT OF KERALA

No. IT-C2/155/2023-ITD

Electronics & Information Technology (C) Department
12-03-2024,Thiruvananthapuram

CIRCULAR

Sub: General security guidelines to all Government organisations to ensure cyber security and to reduce the risk of cyber-attacks – reg

Ref: Letter numbered SDC/11/2023-KSITM dated 12/05/2023 from Director, KSITM

All the Government organisations/departments are requested to strictly comply with the general security guidelines listed below to ensure cyber security and to reduce the risk of cyber-attacks.

General security guidelines

I. Best practices for securing Web Applications

1. All the applications which are hosted at the State Data Centers are to be security audited by a CERT-IN empanelled agency. The details of the agencies are available in https://www.certin.org.in website.
2. The periodical security audits should be done by the department concerned using the CERT-IN empanelled agency once in every 2 years or whenever the source code of the application has been significantly modified whichever is earlier.
3. Ensure that the web servers, application framework and their respective CMS (Content Management System), 3rd party plugins etc., are updated with the latest versions.
4. Sensitive data should always be transferred to the server over an encrypted connection which includes communication between internal components, and with any APIs for external communication,etc.
5. It is recommended to use TLS 1.3 or higher. Disable older protocols (like TLS 1.1, 1.0, SSLV3 etc) in the server. Use Strong Ciphers like AES, GCM, SHA and disable weak ciphers like DES, 3DES, RC4 (or its variants).
6. All passwords, connection strings, tokens, keys etc., should be encrypted with salted hash. There should not be any plain passwords stored in configuration files or source code or in database.

7. Ensure input validation and parameterized queries including prepared statements to protect against SQL injection attacks.
8. Prevent Cross Site Scripting (XSS): Implement HTML/Attribute/JavaScript/CSS/URL Escaping techniques before inserting untrusted Data into web application.
9. Do not expose session ID in the URL.
10. Implement token-based system that changes on every web- request in application, to prevent Cross-Site Request Forgery (CSRF).
11. Prevent Arbitrary File Upload-The file types allowed to be uploaded should be restricted to only those that are necessary for the application functionality. Never accept a filename and its extension directly without having a white list filter. Also please ensure the following recommendations to prevent file upload vulnerability.

- Deny Execute file permissions for uploads directory.
- Limit the filename length.
- Rename the files that are uploaded.
- Use randomly generated filenames for uploaded files.
- Check for the correct MIME type of file before uploading.
- The application should perform filtering and content checking on any files which are uploaded to the server.

12. All exceptions should be handled with displaying custom error pages for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.
13. Directory traversal/listing should be disabled in the web servers. In case of any specific attempt by a user to access a portion of the code by typing the URL path then the same should be redirected to a custom error page.
14. Remove unwanted scripts and executable code from the web server application root directory. Also ensure that backup files are not present within web roots.
15. HTTP Response Headers should be masked. HTTP Only Cookies should be enabled, to restrict access to cookies.

II. Best practices for securing Servers

1. Keep the Operating systems, Databases, Web & Application servers up to date with the latest software versions, minor or major upgrades/patches to protect against the known vulnerabilities.
2. Departments shall ensure that the servers are protected with an Antivirus solution.
3. Make sure that a dedicated User account with limited privileges should be

used for the Web Server Processes. The Web Server processes should not be running under Administrator/Admin or Root user Account.

4. Use only complex passwords (with minimum 8 characters length with a combination of numbers, upper case & lower case letters, special characters etc.) for all the servers. The password shall be changed at least once in every 3 months.
5. Internet access should be limited in the servers and only authorized URLs to be white listed in the case of using external API's.
6. Remove or disable unwanted users, groups, services and ports etc. in the servers.
7. The configuration files of the web server should be given read only access by web server process.
8. Remove the web server banner information so that web server and operating system type and version are not reported.
9. Remove all sample files scripts, manuals and executable code from the web server application root directory.
10. All default user names and IIS/apache pages (like admin, default.aspx, index.aspx...etc) should be renamed.
11. An account lockout feature shall be enabled on the server access via SSH, (max 5 incorrect attempts) or through group policy in Windows servers.
12. The HTTP Strict-Transport-Security response header (HSTS) shall be enforced. Any "non-https" requests received on the website/applications, should be forcefully re-directed to "https".
13. Periodical backups have to be taken for the critical applications by the Departments. Local backups also to be maintained in a secure manner (Ideally data should be kept on a separate device, and backups should be stored offline in a secure manner).
14. Access Logs, Error logs, Audit logs and secure logs should be enabled on the servers. In case of Cloud VMs, the department should keep the logs at least for a period of 15 days in the local servers. Also maintain the backup of logs for a period of 3 months and same should be readily available for any incident investigation.
15. If the applications are hosted at State Data Centres, syslogs should be forwarded to the SIEM (Security Information and Event management) solution of State Data Centre. The departments can send an email to sdc.ksitm@kerala.gov.in. for forwarding logs to the SIEM.
16. Regularly review the server log files (Access/Error/Security logs) for knowing any attacks and intrusions, preferably daily. If any security breaches noticed, the same should be reported to cert.ksitm@kerala.gov.in (Logs with HTTP error code 403 (Forbidden) and 404 (Not found) may be

malicious attempts).

17. Use web application firewall / iptables for monitoring/ filtering the request in order to prevent hacking attempts.
18. Departments/Application developers shall review their firewall rules and user accounts (e.g.,username & password) on a periodic basis at least once in a month.
19. Application developers / Departments shall use VPN connection provided by State Data Centre for connecting remotely to their servers.

III. Best practices for securing Desktops / Laptops

1. All the computers should be installed with the genuine Operating Systems, Antivirus and should be updated with latest security patches.
2. Keep the web browsers and the plugins updated with the latest versions.
3. Always protect the computers with strong passwords.
4. Use of peer-to-peer network applications like torrent, pirated software etc., are prohibited as these are common sources of malware and viruses.
5. Limit the usage of USB Storage devices. Always scan USB storage devices with latest Antivirus before accessing.
6. Ensure that the "REMEMBER PASSWORD" option isn't configured anywhere, i.e in the browser or in POP client such as outlook, thunder bird etc. Otherwise remove all the saved passwords and change the configuration.
7. The passwords should be changed periodically.
8. Encourage users to be cautious while browsing internet – not to download files from untrusted sites.
9. Be cautious while checking emails – not to open spam/ suspicious emails which may download malicious content.
10. Ensure backup for the important files to external storage devices.
11. Logs should be stored and same should be readily available for incident investigation.

Yours Faithfully,
DR RATHAN U KELKAR I A S
SECRETARY
For Secretary to Government.

Copy to:

All Government departments & organisations

Stock file/Office copy

Signed by
Smitha A.s
Date: 13-03-2024 16:58:52

I/6109747/2024

Forwarded/By Order,

Section Officer.