GOVERNMENT OF SIKKIM
DEPARTMENT OF INFORMATION TECHNOLOGY
Secretariat Annexe-I, Sonam Tshering Marg
Gangtok, Sikkim

Email id: secy-dit-sik@nic.in

visit us at: www.sikkim.gov.in

Subject: *Advisory measures for prevention of web intrusion attacks/ web defacement.*

The National Cyber Coordination Centre (NCC) has reported that the websites of state and central government are being potentially targeted hacker groups with DoS/DDoS attacks, claiming to target 12000 critical Government websites and other Government IT Infrastructure of India in their fresh set of attacks. In this regard, it is advised to take the following measures for prevention of web intrusion attacks/web defacement:

1. Use latest version of Web server, Database Server, Hypertext Processor (PHP).
2. Apply appropriate updates/patches on the OS and Application software.
3. Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug the vulnerabilities found.
4. Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
5. Enable and maintain logs of different devices and servers and maintain the same for all the levels.
6. Use Web Application Firewall (WAF), Security Information and Event Management (SIEM) and/or Database Activity Monitoring (DAM) solutions.
7. Search all the websites hosted on the web server or sharing the same DB server for the malicious web shells or any other artefact.
8. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed.
9. In order to identify web shells, scan the server with Yara rules.
10. Change database passwords of all the accounts available in the compromised database server. Also, change the passwords/credentials stored in the databases present on the database server.
11. Use an application firewall to control input, output and/or access to the web application.
12. Limit the file types allowed to be uploaded to the web server by using a list of predetermined file types. Define permissions on the directory files are uploaded into, to prevent attackers from executing the files after upload.
13. Consider using File Integrity Monitoring (FIM) solution on web servers to identify unauthorized changes to files on the server.

The following lists of websites are hereby advised to strictly follow the above measures.

LIST OF WEBSITES SUBMITTED BY NCCC, CERT-IN:

sikkim-vigilance.gov.in	sikkimagrisnet.org
sikkim.data.gov.in	www.sikkimassembly.org
sikkimcrafts.gov.in	www.sikkimhrdd.org
sikkimeccl.gov.in	www.sikkimstdc.com
sikkimfcs-cad.gov.in	www.powerdepartmentsikkim.com
sikkimfred.gov.in	www.nitsikkim.ac.in
sikkimlrdm.gov.in	www.sikkim.nic.in
sikkimmines.gov.in	www.sikenvis.nic.in
sikkimtax.gov.in	sikkimslsa.nic.in
sikkimtender.gov.in	sikkimpolice.nic.in
sikkimtourism.gov.in	sikkimjudicialacademy.nic.in
spscskm.gov.in	sikkim.nic.in
www.attc.skmpoly.edu.in	ceosikkim.nic.in
www.ccct.skmpoly.edu.in	www.sikkim-excise.gov.in
secsikkim.org	www.sikkim-roadsandbridges.gov.in
rajbhavansikkim.gov.in	www.sikkimforest.gov.in
bioinformaticssikkim.gov.in	www.imdsikkim.gov.in