NIC-CERT/2023-09/EA-2
Dated: 06-09-2023
Severity Level: HIGH

Emergency Security Alert in view of G20 Summit New Delhi

A. Description

The G20 Summit will be held on 9th & 10th September 2023 in New Delhi. The global nature of the G20 Summit makes it a high-profile target for malicious cyber threat actors. The objectives of these potentially harmful actors could span from trying to disrupt essential services, obstruction of crucial networks, phishing attacks and defacement of govt. websites and applications with the intention of causing embarrassment or using the moment to propagate malicious narratives and disinformation.

B. Cyber Security precautions to be undertaken

In view of the above, heightened cybersecurity vigilance is essential. It is strongly recommended that the following measures be undertaken by respective NIC application owners and their Third Party/ contractual manpower who are involved in the development, design, testing, implementation, audit, operations, management and troubleshooting of any Government Infrastructure/Services:

- It is advised that the sites that are not security audited, despite reminders, should be restricted to be accessed from internet and only allowed from NICNET after consultation with the respective CISO of the ministry/departments.
- Ensure that all the sites and applications that are not SSL-enabled should be enabled with valid SSL certificate. Urgent actions need to be initiated for the compliance of the same.
- Ensure that the Websites, Applications and Databases are monitored round the clock for any unauthorized changes or modifications. Officials to be deployed 24x7 for monitoring of the critical assets/applications/webservers.
- Ensure that proper logging is enabled in all servers and logs are being monitored for any unusual or suspicious activities.
- Restrict the access of CMS/Site Administration Access to NIC's VPN based IPs only. These Admin URLs should not be accessible over the internet.
- Change all administrator credentials for Servers, Databases, Applications, Content Management Systems and other management components as per the policy.
- Ensure that proper security hardening is carried out on all servers i.e. webservers, databases etc. To be ensured immediately.
- Take prompt action on security advisories/alerts published by NIC-CERT/Cyber Security Group/Audit Group.

In case of any security incident kindly report it to NIC-CERT at:
incident@nic-cert.nic.in