BGD e-GOV CIRT

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

04 June 2025

Situational Awareness for Eid-ul-Adha Holidays

BGD e-GOV CIRT, BCC remains committed to proactively securing the nation's cyberspace. As the extended Eid holidays approach, we anticipate an increased risk of cyberattacks, as malicious actors often exploit periods of reduced monitoring and operational oversight. Our Cyber Threat Intelligence Unit has already identified widespread malware activity, including strains such as **Android.vo1d** and **Avalanche-Andromeda**, which have compromised thousands of IP addresses nationwide.

In addition to active malware campaigns, numerous systems remain highly vulnerable due to weak authentication practices, outdated software and services, unpatched critical vulnerabilities, etc., that enable Remote Code Execution (RCE). These vulnerabilities substantially increase the risk of data breaches, ransomware attacks, unauthorized system access, and more. We strongly urge all public and private sector entities to reinforce their cybersecurity posture, particularly during the upcoming holidays, by applying necessary patches, strengthening authentication mechanisms, and maintaining vigilant monitoring.

In the past week alone, **24,362 IPs** showed vulnerabilities, and **370,508 IPs** were infected with malware, indicating a heightened risk of exploitation.

Figure: Top 10 Malware and Exposed Vulnerabilities in Bangladesh [last week]

We urge all entities in Bangladesh to implement the following measures to strengthen the security of their infrastructure:

- Ensure continuous 24/7 monitoring of systems, networks, and user activities.
- Keep all security tools (SIEM, IDS/IPS, WAF) active and updated to detect and prevent threats.
- Allow remote access only via approved VPNs with Multi-Factor Authentication.
- Block access from public or untrusted networks.
- Prohibit the use of outdated or unpatched software; apply all critical updates.
- Maintain secure backups of essential systems and test recovery procedures.
- Temporarily restrict non-essential access and disable unused or inactive accounts.
- Report any IOCs or suspicious activity to BGD e-GOV CIRT at cti@cirt.gov.bd or cirt@cirt.gov.bd