BGD e-GOV CIRT

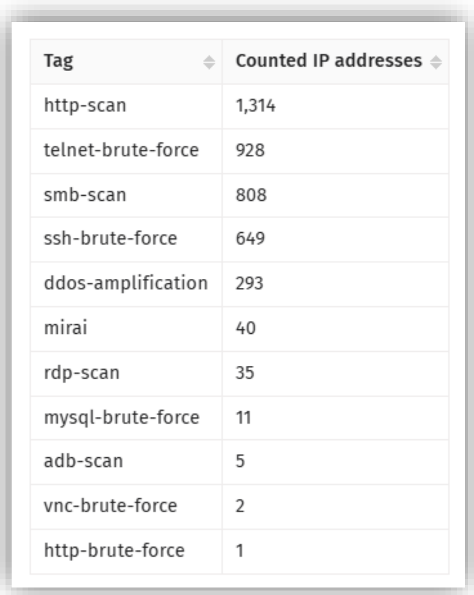
BANGLADESH
COMPUTER
COUNCIL
COMPUTER FOR EVERYTHING

27 March 2025

Situational Awareness for Eid Holidays

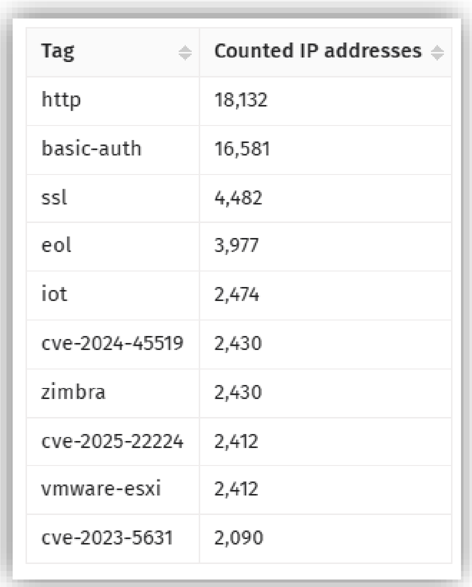
The Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT), BCC is working to protect the nation’s cyberspace by proactively managing computer security incidents and related threats. As the long Eid holidays approach, cybercriminals may attempt to exploit security gaps due to reduced monitoring and response capabilities. The CTI unit of BGD e-GOV CIRT has recently detected multiple web-based attack attempts, particularly targeting non-office hours and weekly holidays. Prominent web attack patterns include SSH brute force, SQL injection, PHP CGI-bin exploits, and directory traversal attacks, all aiming for unauthorized access or exploitation.

Additionally, in the **past week**, several cyberattacks have been observed targeting Bangladesh. Notably, **26,887 IP addresses** were identified with one or more exposed vulnerabilities, increasing the risk of exploitation.



Tag	Counted IP addresses
http-scan	1,314
telnet-brute-force	928
smb-scan	808
ssh-brute-force	649
ddos-amplification	293
mirai	40
rdp-scan	35
mysql-brute-force	11
adb-scan	5
vnc-brute-force	2
http-brute-force	1

Figure: Identified attack attempts



Tag	Counted IP addresses
http	18,132
basic-auth	16,581
ssl	4,482
eol	3,977
iot	2,474
cve-2024-45519	2,430
zimbra	2,430
cve-2025-22224	2,412
vmware-esxi	2,412
cve-2023-5631	2,090

Figure: Top 10 exposed vulnerabilities

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

- Maintain 24/7 system and network monitoring.
- Keep security tools (SIEM, IDS/IPS, WAF) active to detect threats.
- Use only approved VPN and MFA for external access.
- Restrict connections from public or unsecured networks.
- Prohibit outdated or unpatched software.
- Maintain secure backups of critical data and be prepared to activate disaster recovery protocols.
- Restrict unnecessary access, especially during holidays and disable unused or temporary accounts.
- Report incidents to relevant cybersecurity authorities. You may inform the detection of IOCs and/or any suspicious activities you observe within your environment, to BGD e-GOV CIRT through email: cti@cirt.gov.bd or cirt@cirt.gov.bd