**Cyber Security Advisories**

**Date: 28 March 2025**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | TA-PHI-2025-03-06-001 Phishing Attack |  |  |  |
|  | TA-APT-2025-03-06-001 CrimsonRAT-  APT36 Campaign |  |  |  |
|  | VA-2025-03-06-001 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-03-07-001 Squidoor Malware |  |  |  |
|  | TA-PHI-2025-03-07-002 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2025-03-07-002 APT Space Pirates |  |  |  |
|  | TA-PHI-2025-03-07-003 Phishing Attack |  |  |  |
|  | TA-APT-2025-03-07-003 APT41 also known as Brass Typhoon |  |  |  |
|  | TA-MAW-2025-03-07-002 PlugX Malware |  |  |  |
|  | TA-MI-2025-03-07-001 Malicious IOCs |  |  |  |
|  | TA-MI-2025-03-10-002 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Advisory No: TA-APT-2025-03-10-004  APT Gamaredon |  |  |  |
|  | TA-MAW-2025-03-10-003 SAGARUNEX BACKDOOR MALWARE |  |  |  |
|  | TA-MAW-2025-03-10-004 POLYGLOT MALWARE |  |  |  |
|  | VA-2025-03-10-002  Active Exploitation of Critical Vulnerabilities |  |  |  |
|  | TA-PHI-2025-03-10-004 Malicious Domain Spoofing CERT-In's Domain |  |  |  |
|  | TA-PHI-2025-03-10-005 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-03-10-003 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2025-03-10-006 Phishing Attack |  |  |  |
|  | TA-MAW-2025-03-10-005 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2025-03-11-007 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-03-11-004 Prominent Vulnerability List |  |  |  |
|  | TA-PHI-2025-03-11-008 Phishing Attack |  |  |  |
|  | TA-PHI-2025-03-11-009  Phishing Attack |  |  |  |
|  | TA-PHI-2025-03-12-010 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2025-03-12-005 APT Group SideWinder |  |  |  |
|  | TA-MAW-2025-03-12-006 XCSSET Malware |  |  |  |
|  | TA-PHI-2025-03-13-011 Phishing Attack |  |  |  |
|  | TA-MI-2025-03-13-003 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | VA-2025-03-13-005 Prominent Vulnerability List |  |  |  |
|  | VA-2025-03-13-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2025-03-17-012 Phishing Attack |  |  |  |
|  | TA-MI-2025-03-17-004 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-03-17-013  Business Email Compromise (BEC) Campaign |  |  |  |
|  | TA-PHI-2025-03-18-014 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-TAG-2025-03-18-001 Threat Actor Group UNC3886 Targeting Juniper Routers |  |  |  |
|  | TA-APT-2025-03-18-006 APT 15 aka Mirage |  |  |  |
|  | TA-MAW-2025-03-18-007 KOSPY SPYWARE and ROKRAT Malware |  |  |  |
|  | VA-2025-03-20-007 CVE-KB Correlation |  |  |  |
|  | VA-2025-03-20-009 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | VA-2025-03-20-008 Active Exploitation of Apache Tomcat Vulnerability |  |  |  |
|  | TA-MI-2025-03-21-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-TAG-2025-03-21-002 Presence of Unknown Threat Actor in Indian CyberSpace |  |  |  |
|  | TA-MAW-2025-03-21-009 POISONPLUG (aka ShadowPad) Malware |  |  |  |
|  | TA-MAW-2025-03-21-010 SOGU aka PLUGX Malware |  |  |  |
|  | TA-MI-2025-03-25-006 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-03-25-016 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-03-25-011 Prominent Vulnerability List |  |  |  |
|  | TA-APT-2025-03-25-007 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-APT-2025-03-25-008 APT SideCopy |  |  |  |
|  | TA-APT-2025-03-25-009 APT FishMonger |  |  |  |
|  | TA-PHI-2025-03-27-017 Phishing Attack |  |  |  |
|  | TA-PHI-2025-03-27-018 Malicious Domains used by Threat Actors |  |  |  |