**Cyber Security Advisories**

**Date: 16 December 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | TA-PHI-2024-12-04-001 Phishing Attack |  |  |  |
|  | TA-APT-2024-12-04-002 APT 19 |  |  |  |
|  | TA-APT-2024-12-04-001 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-MAW-2024-12-04-001 Weekly Mirai Activity Report |  |  |  |
|  | VA-2024-12-05-001 CVE - KB Correlation |  |  |  |
|  | TA-MAW-2024-12-06-002 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-TAG-2024-12-06-001 State-Sponsored Threat Actor's Cyber-Espionage Campaigns |  |  |  |
|  | TA-APT-2024-12-06-003 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-PHI-2024-12-06-002 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-12-06-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-RAN-2024-12-10-001 Ransomware Attack by Executing HRSword Tool |  |  |  |
|  | TA-PHI-2024-12-10-003 Phishing Attack |  |  |  |
|  | TA-MAW-2024-12-10-003 Malicious IOCs |  |  |  |
|  | TA-MAW-2024-12-11-004 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2024-12-11-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-12-11-002 Ransomware Attack by Executing HRSword Tool |  |  |  |
|  | TA-MAW-2024-12-11-006 DOGCALL MALWARE |  |  |  |
|  | TA-MAW-2024-12-11-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-12-12-007 Exfiltration Risk from PowerSCP Stealer |  |  |  |
|  | TA-MAW-2024-12-13-008 Threat Actors Using Legitimate Web Services/APIs for Data Exfiltration |  |  |  |
|  | TA-PHI-2024-12-13-005 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-12-13-004 Active Exploitation of a Critical Flaw (CVE-2024-50623) Affecting CLEO's File Transfer Products |  |  |  |