**Cyber Security Advisories**

**Date: 15 November 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | TA-MAW-2024-10-30-23 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-RAN-2024-11-04-001 Interlock Ransomware |  |  |  |
|  | TA-RAN-2024-11-04-002 State-Sponsored Malware Campaign Targeting Critical Sectors |  |  |  |
|  | TA-APT-2024-11-04-001 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-PHI-2024-11-05-001 ClearFake Malware Framework |  |  |  |
|  | TA-PHI-2024-11-05-002 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-11-05-002 APT 36 using CrimsonRAT Malware |  |  |  |
|  | VA-2024-11-05-001 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2024-11-06-003 Phishing Attack |  |  |  |
|  | TA-PHI-2024-11-06-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-11-07-003 Lynx Ransomware |  |  |  |
|  | TA-MAW-2024-11-08-001 Weekly Mirai Activity Report |  |  |  |
|  | TA-TAG-2024-11-08-001 TAG-110 aka UAC-0063 and Bluedelta |  |  |  |
|  | VA-2024-11-08-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-APT-2024-11-11-003 SideCopy Malware C&C IP |  |  |  |
|  | TA-APT-2024-11-11-004 APT 36 using Eliza RAT Malware |  |  |  |
|  | TA-PHI-2024-11-11-005 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-11-11-004 State-Sponsored Malware Campaign Targeting Critical Sectors |  |  |  |
|  | VA-2024-11-12-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | VA-2024-11-12-007 Security Updates for  Palo Alto Network  product Expedition |  |  |  |
|  | TA-APT-2024-11-13-005 APT 36 Deploying ActionRAT Malware |  |  |  |
|  | TA-PHI-2024-11-13-006 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-11-13-008 Critical Vulnerabilities in Multiple Products |  |  |  |