**Cyber Security Advisories**

**Date: 16 September 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-2024-08-30-28 Fabookie Infostealer |  |  |  |
|  | TA-MAW-2024-08-30-029 PG\_MEM  Malware |  |  |  |
|  | TA-RAN-2024-09-02-001 Ransom Hub Ransomware |  |  |  |
|  | TA-MAW-2024-09-03-001 Cheana Stealer |  |  |  |
|  | TA-MAW-2024-09-04-002 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-04-003 Sedexp Malware |  |  |  |
|  | VA-2024-09-04-001 ACTIVE EXPLOITATION OF PUBLIC FACING APPLICATION VULNERABILITIES |  |  |  |
|  | TA-MAW-2024-09-04-004 Malicious IPs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-05-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-05-006 ToneShell Malware Campaign |  |  |  |
|  | VA-2024-09-06-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2024-09-06-01 Phishing Domains |  |  |  |
|  | TA-MAW-2024-09-06-007 Malicious IOCs |  |  |  |
|  | TA-PHI-2024-09-13-02 Phishing Attack |  |  |  |
|  | TA-PHI-2024-09-13-03 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-09-13-001 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-RAN-2024-09-13-002 Cicada3301 Ransomware |  |  |  |
|  | TA-MAW-2024-09-13-008 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-09-13-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-09-13-002 SideCopy Malware C&C IP |  |  |  |
|  | TA-RAN-2024-09-13-003 BlackByte Ransomware |  |  |  |
|  | TA-MAW-2024-09-13-009 Linux Malware C&C Domain and IP |  |  |  |