**Cyber Security Advisories**

**Date: 30 August 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-P-082024094 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-0820240704 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-995082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P082024062 Dispossessor Ransomware |  |  |  |
|  | CMTX-P082024007 SystemBC Malware Campaign |  |  |  |
|  | CMTX-I-514082024 SideCopy Malware C&C IP |  |  |  |
|  | CMTX-P082024095 QWERTY INFO STEALER |  |  |  |
|  | CMTX-P082024104 Beavertail Malware Campaign |  |  |  |
|  | CMTX-P-5870820249 Threat Actor Group-110 (TAG 110) Recent IOCs |  |  |  |
|  | CMTX-I-445082024 CrimsonRAT Malware C&C IP |  |  |  |
|  | CMTX-P082024115 CVE-2024-38193 |  |  |  |
|  | CMTX-I-587082024 Suspicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-765082024 Malicious Domain used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P082024956 Styx Stealer |  |  |  |
|  | CMTX-I-995082024 Malicious/ Suspicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-082024114  RedJuliett Threat Actor Campaign |  |  |  |
|  | CMTX-P-082024125 STORMBAMBOO THREAT ACTOR CAMPAIGN |  |  |  |
|  | CMTX-P082024108 REDLINESTEALER Malware Campaign |  |  |  |
|  | CMTX-P-082024135 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-082024145 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-680082024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-636082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-179082024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-432082024 Android RAT Latest C&C IP |  |  |  |
|  | CMTX-P-082024155 VELVETSHELL MALWARE |  |  |  |
|  | CMTX-P082024834 MoonPeak Malware Campaign |  |  |  |
|  | CMTX-I-781082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P082024976 QuasarRAT Malware |  |  |  |
|  | CMTX-P082024664 Ransom Hub Ransomware |  |  |  |
|  | CMTX-P082024165 ACTIVE EXPLOITATION OF PUBLIC FACING APPLICATION VULNERABILITIES BY IRANIAN THREAT ACTORS |  |  |  |
|  | CMTX-I-950082024 QuasarRAT- Deployed by Pakistan based Threat Actors |  |  |  |
|  | TA-PHI-2024-08-16-001 Phishing Domains |  |  |  |
|  | TA-MAW-2024-08-16-013 Spark RAT Malware Campaign |  |  |  |
|  | TA-MAW-2024-08-16-12 Quad7 Botnet |  |  |  |
|  | TA-MAW-2024-08-16-009 AsyncRAT Malware |  |  |  |
|  | TA-APT-2024-08-16-002 Earth Baku Threat Actor Campaign |  |  |  |
|  | TA-MAW-2024-08-16-010 SolarMarker RAT Malware Campaign |  |  |  |
|  | TA-RAN-2024-08-16-009 LOSTINFO RANSOMWARE |  |  |  |
|  | TA-MAW-2024-08-19-014 Dark Crystal RAT (DC RAT) |  |  |  |
|  | VA-2024-08-21-004 CRITICAL VULNERABILITIES IN OPENSSH |  |  |  |
|  | VA-2024-08-21-005 Critical RCE Vulnerability in WordPress Websites |  |  |  |
|  | TA-MAW-2024-08-21-16 SystemBC Malware Campaign |  |  |  |
|  | TA-PHI-2024-08-21-002 Phishing Attack |  |  |  |
|  | TA-MAW-2024-08-22-018 Beavertail Malware Campaign |  |  |  |
|  | TA-RAN-2024-08-22-010 Dispossessor Ransomware |  |  |  |
|  | VA-2024-08-22-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-08-23-019 Fenix Botnet |  |  |  |
|  | TA-PHI-2024-08-23-003 Phishing Attack |  |  |  |
|  | TA-MAW-2024-08-23-20 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-08-23-021 QWERTY Information Stealer |  |  |  |
|  | VA-2024-08-23-007 Threat Actors Exploiting Elevation of Privilege Vulnerability in Microsoft Windows Systems |  |  |  |
|  | TA-PHI-2024-08-23-004 Credential Theft Phishing Campaign |  |  |  |
|  | TA-MAW-2024-08-27-022 Malicious IOCs related to Shadowpad Malware |  |  |  |
|  | TA-RAN-2024-08-27-011 Ransomware Targeting Critical Information Infrastructures (CIIs) |  |  |  |
|  | TA-PHI-2024-08-27-005 Phishing Attack |  |  |  |
|  | TA-MAW-2024-08-27-023 Styx Stealer |  |  |  |
|  | VA-2024-08-28-008 CVE - KB Correlation, Aug 2024 |  |  |  |
|  | TA-MAW-2024-08-28-025 REDLINESTEALER Malware Campaign |  |  |  |
|  | TA-MAW-2024-08-28-024 VELVETSHELL MALWARE |  |  |  |
|  | TA-MAW-2024-08-28-026 MoonPeak Malware Campaign |  |  |  |
|  | VA-2024-08-28-009 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-08-29-027 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-08-29-006 Threat Actors using Business Email Compromise (BEC) attacks |  |  |  |
|  | TA-PHI-2024-08-29-007 Phishing Domains |  |  |  |
|  | TA-TAG-2024-08-29-003 Threat Actors targeting Internet Service Providers (ISPs) Networks |  |  |  |