**Cyber Security Advisories**

**Date: 30 October 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-I-636102024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-P-102024144 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024154 PlugX Malware Campaign |  |  |  |
|  | CMTX-P102024164 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024045 MYTHIC Malware Campaign |  |  |  |
|  | CMTX-P-8650920249 Threat Actor Group (TAG)-102- Advanced Cyber Espionage Group |  |  |  |
|  | CMTX-I-335102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-345102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-2521020249 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-102024174 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-8211020249 Redline Malware Alert |  |  |  |
|  | CMTX-P-102024184 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-9271020249 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-7781020249 Amadey Malware Alert |  |  |  |
|  | CMTX-P-8701020249 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-I-845102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-850102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-8851020249 Supershell Malware |  |  |  |
|  | CMTX-P102024055 Adversary-in-the-middle (AiTM) Phishing Attack Bypass MFA |  |  |  |
|  | CMTX-P102024065 FORTINET VULNERABILITIES |  |  |  |
|  | CMTX-P102024075 CRITICAL VULNERABILITIES IN IVANTI PRODUCTS |  |  |  |
|  | CMTX-I-420102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-102024194 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-102024204 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024085 ACTIVE EXPLOITATAION OF A CRITICAL FLAW (CVE-2024-9680) AFFECTING FIREFOX AND FIREFOX EXTENDED SUPPORT RELEASE (ESR) |  |  |  |
|  | CMTX-P102024214 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P102024095 ACTIVE EXPLOITATION OF A CRITICAL VULNERABILITY (CVE-2024-28987) AFFECTING SOLARWINDS HELP DESK SOFTWARE |  |  |  |
|  | CMTX-I-650102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-514102024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-P-102024105 Interlock Ransomware Activity |  |  |  |
|  | TA-APT-2024-10-17-007 State-Sponsored Groups or Cybercriminal Organizations Targeting Various Sectors |  |  |  |
|  | TA-MAW-2024-10-18-011 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2024-10-18-008 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-10-18-009 Threat Actors Hiding Malicious Phishing Pages Behind Legitimate CAPTCHAs |  |  |  |
|  | TA-PHI-2024-10-18-010 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-10-21-008 Malicious IPs used by APT 36 & State Sponsored Threat Actors |  |  |  |
|  | VA-2024-10-21-010 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-10-23-13 Unknown Malware Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-10-23-011 Phishing Attack |  |  |  |
|  | TA-PHI-2024-10-24-13 AiTM Phishing Attack Techniques Circumvents MFA to Conduct Identity-Based Attacks |  |  |  |
|  | TA-PHI-2024-10-24-12 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-10-24-14 UAC-0050's Phishing Campaign to Deploy Remcos RAT |  |  |  |
|  | TA-APT-2024-10-24-007 APT Group IcePeony |  |  |  |
|  | TA-MAW-2024-010-24-014 Redline Stealer Malware |  |  |  |
|  | VA-2024-10-24-011 Active  Exploitation of VBR Server Critical Deserialization Vulnerability to Deploy Akira & Fog Ransomware |  |  |  |
|  | TA-PHI-2024-10-25-015 Phishing Attack |  |  |  |
|  | TA-MAW-2024-010-25-015 Trickbot Malware |  |  |  |
|  | TA-MAW-2024-10-25-016 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | VA-2024-10-25-017 FORTINET VULNERABILITIES |  |  |  |
|  | TA-MAW-2024-10-28-017 Agent Tesla Malware |  |  |  |
|  | TA-MAW-2024-10-28-018 Amadey Malware |  |  |  |
|  | TA-MAW-2024-10-28-019 SocGholish Malware |  |  |  |
|  | TA-PHI-2024-10-28-016 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-10-28-012 CVE - KB Correlation |  |  |  |
|  | TA-MAW-2024-10-28-020 Supershell Malware |  |  |  |
|  | VA-2024-10-29-013 CRITICAL VULNERABILITIES IN IVANTI PRODUCTS |  |  |  |
|  | TA-MAW-2024-10-29-021 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2024-10-29-022 Unknown Malware Targeting Critical Sectors |  |  |  |