**Cyber Security Advisories**

**Date: 15 January 2025**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-I-443012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-080012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-012025024 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-012025014 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-012025015 Beast Ransomware |  |  |  |
|  | CMTX-I-021012025 Mythic Malware- Pakistan Based Malware Campaign |  |  |  |
|  | CMTX-I-025012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-012025034 PLUGX Malware Campaign |  |  |  |
|  | CMTX-P-012025044 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-028012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-911012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-VUL-0120256615 Prominent Vulnerability List |  |  |  |
|  | CMTX-P012025105 CRITICAL VULNERABILITIES AFFECTING IVANTI CONNECT SECURE VPN APPLIANCES |  |  |  |
|  | CMTX-P-012025905 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-012025915 PlugX Malware Campaign |  |  |  |
|  | CMTX-P012025205 A CRITICAL RCE FLAW (CVE-2024-52875) AFFECTING GFI KERIOCONTROL FIREWALLS , (TLP: CLEAR) |  |  |  |
|  | CMTX-I-032012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-6080120259 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-9590120259 Ursnif Malware Alert |  |  |  |
|  | CMTX-P-9130120259 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-1750120259 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-5530120259 Redline Malware Alert |  |  |  |
|  | CMTX-P-7360120259 Amadey Malware Alert |  |  |  |
|  | CMTX-P-6110120259 Emotet Malware Alert |  |  |  |
|  | CMTX-P-2930120259 Raccoon Stealer Malware Alert |  |  |  |
|  | CMTX-I-781012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-445012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P012025204 FunkSec Ransomware |  |  |  |
|  | TA-APT-2025-01-02-001 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-PHI-2025-01-02-001 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2025-01-02-00 Phishing Attack |  |  |  |
|  | TA-PHI-2025-01-02-003 Malware Targeting Government Officials via Spear-Phishing |  |  |  |
|  | TA-MAW-2025-01-02-001 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-01-03-003 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-01-03-001 CVE - KB Correlation, Dec 2024 |  |  |  |
|  | VA-2025-01-03-002 Prominent Vulnerability List |  |  |  |
|  | TA-APT-2025-01-03-002 Salt Typhoon |  |  |  |
|  | TA-PHI-2025-01-07-004 Phishing Attack |  |  |  |
|  | TA-PHI-2025-01-08-005 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2025-01-08-001 Beast Ransomware |  |  |  |
|  | TA-MAW-2025-01-10-002 Mythic Malware |  |  |  |
|  | VA-2025-01-10-003 Prominent Vulnerability List |  |  |  |
|  | TA-PHI-2025-01-10-006 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-10-003 NetSupport RAT campaign |  |  |  |
|  | TA-MAW-2025-01-10-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2025-01-10-004 Malicious IOCs |  |  |  |
|  | TA-APT-2025-01-13-003 APT15  aka Vixen Panda |  |  |  |
|  | TA-MAW-2025-01-13-006 Winnti Malware |  |  |  |
|  | TA-MAW-2025-01-13-007 SOGU aka PLUGX Malware |  |  |  |
|  | TA-MAW-2025-01-13-008 SPACEHOP aka ORB3 Network |  |  |  |
|  | TA-MAW-2025-01-13-009 POISONPLUG (aka ShadowPad) Malware |  |  |  |
|  | TA-TAG-2025-01-13-001 Presence of Unknown PRC Threat Actor in Indian CyberSpace |  |  |  |
|  | TA-MAW-2025-01-13-010 Presence of NightFall Malware in Indian CyberSpace |  |  |  |
|  | VA-2025-01-13-004 CRITICAL VULNERABILITIES AFFECTING IVANTI CONNECT SECURE VPN APPLIANCES |  |  |  |
|  | TA-PHI-2025-01-14-007 Phishing Attack |  |  |  |
|  | VA-2025-01-14-005 CRITICAL RCE FLAW (CVE-2024-52875) AFFECTING GFI KERIOCONTROL FIREWALLS |  |  |  |
|  | TA-PHI-2025-01-14-007 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-14-011 Agent Tesla Malwar |  |  |  |
|  | VA-2025-01-14-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-01-14-013 Trickbot Malware |  |  |  |
|  | TA-MAW-2025-01-14-012 Ursnif Malware |  |  |  |
|  | TA-MAW-2025-01-14-014 RedLine Malware |  |  |  |
|  | TA-MAW-2025-01-14-015 SocGholish Malware |  |  |  |
|  | TA-PHI-2025-01-15-008 Phishing Attack |  |  |  |