**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** |
|  | CMTX-P-102024224 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024234 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-080112024 Mythic Malware- APT36 campaig |  |  |  |
|  | CMTX-I-0230102024 IOC of suspicious domains used for sending spear phishing mails |  |  |  |
|  | CMTX-P102024115 Active Exploitation of Critical Zimbra Postjournal Flaw (CVE-2024-45519) |  |  |  |
|  | CMTX-P-112024014 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-112024024 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-020112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-112024164 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024174 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-080112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P112024105 ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2024-37383) AFFECTING ROUNDCUBE WEBMAIL |  |  |  |
|  | CMTX-P-112024044 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024034 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P112024054 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-I-404112024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-I-445112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024104 Critical Vulnerability Affecting Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) devices CVE-2024-20481 |  |  |  |
|  | CMTX-I-443112024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-514112024 Eliza RAT Malware- APT36 |  |  |  |
|  | CMTX-I-689112024 Malicious Domains used for Phishing |  |  |  |
|  | CMTX-P-112024184 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P112024205 EXPLOITATION OF A CRITICAL FLAW (CVE-2024-20481) AFFECTING CCISCO FIREPOWER THREAT DEFENSE (FTD) SOFTWARE AND CISCO ADAPTIVE SECURITY APPLIANCE (ASA) SOFTWARE |  |  |  |
|  | CMTX-I-863112024 SideCopy- C&C of Malware Campaign |  |  |  |
|  | CMTX-I-9907112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024405 IMMEDIATE PATCHING REQUIRED FOR ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2024-5910) IN PALO ALTO NETWORK EXPEDITION |  |  |  |
|  | CMTX-P-112024314 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-112024414 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-556112024 ActionRAT Malware- APT36 campaign |  |  |  |
|  | CMTX-P112024984 Relay server Nodes used by Chinese actors--ALERT10 |  |  |  |
|  | CMTX-P-112024214 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-112024224 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-333112024 APT36 campaign |  |  |  |
|  | CMTX-I-214112024 Malicious Domain used by Threat Actors |  |  |  |
|  | CMTX-P-112024018 RustDoor Malware |  |  |  |
|  | CMTX-I-500112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-331112024 AsyncRAT Malware |  |  |  |
|  | CMTX-I-993112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-025112024 SideCopy- C&C of Malware Campaign |  |  |  |
|  | CMTX-P-112024364 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024784 Cumulative Suspicious Domains |  |  |  |
|  | 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 |  |  |  |