**Cyber Security Advisories**

**Date: 17 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-P102024075 Salt Typhoon Activity |  |  |  |
|  | CMTX-I-401102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-400102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024106 Blackout Ransomware |  |  |  |
|  | CMTX-P102024024 INC Ransomware |  |  |  |
|  | CMTX-P-102024034 Dark Crystal RAT (DC RAT) |  |  |  |
|  | CMTX-P102024044 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024174 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024164 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-500102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-502102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024054 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024064 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-102024074 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024084 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-301102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-302102024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-053102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-053102024\_1 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-P-102024034 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-587102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-502102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-137102024 SideCopy Malware C&C Domain |  |  |  |
|  | CMTX-P102024094 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P102024104 RCRU64 Ransomware |  |  |  |
|  | CMTX-I-025102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-021102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-102024015 Critical Alert: MYTHIC Malware Campaign |  |  |  |
|  | CMTX-I-069102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024114 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024124 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024134 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-080102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-102024025 ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE |  |  |  |
|  | CMTX-I-808102024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-102024025 ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE |  |  |  |
|  | CMTX-P102024035 ACTIVE EXPLOITATION OF IVANTI CLOUD SERVICE APPLIANCE(CSA)FLAWS BY NATION STATE ADVERSARY |  |  |  |
|  | CMTX-I-443102024 SideCopy Malware C&C IP |  |  |  |
|  | CMTX-I-665102024 Malicious Domains used for Phishing |  |  |  |
|  | CMTX-I-389102024 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-10-01-002 Remote Command Execution Vulnerability (CVE-2024-45519) in Zimbra Collaboration Suite |  |  |  |
|  | TA-MAW-2024-10-01-001 SocGholish Activity |  |  |  |
|  | TA- APT-2024-10-001 Salt Typhoon Activity |  |  |  |
|  | VA-2024-10-01-001 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-10-03-002 ClearFake Malware Framework |  |  |  |
|  | TA-PHI-2024-10-03-001 Threat actors using API of Popular Messaging and Meeting Applications for Phishing and Malware Campaign |  |  |  |
|  | TA-MAW-2024-10-03-003 Dark Crystal RAT (DC RAT) |  |  |  |
|  | TA-APT-2024-10-03-002 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-PHI-2024-10-04-002 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-10-04-001 INC Ransomware |  |  |  |
|  | TA-MAW-2024-10-04-004 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | VA-2024-10-07-003 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-10-07-005 Threat actors using ChromeLoader and Associated Adware Leverages MSI files Masquerading as PDF Software |  |  |  |
|  | TA-RAN-2024-10-08-002 Blackout Ransomware Group |  |  |  |
|  | TA-APT-2024-10-08-003 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-PHI-2024-10-08-003 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-10-08-004 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-TAG-2024-10-08-001 Threat Actor Z-BL4CX-H4T |  |  |  |
|  | TA-MAW-2024-10-08-006 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-10-09-007 Weekly Mirai Activity Report |  |  |  |
|  | TA-APT-2024-10-09-004 APT 36 using CrimsonRAT Malware |  |  |  |
|  | VA-2024-10-09-005 Critical OS Command Injection Vulnerability Affecting Linear eMerge e3-Series Products |  |  |  |
|  | TA-PHI-2024-10-09-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-10-10-005 Mythic Malware- APT36 Campaign |  |  |  |
|  | VA-2024-10-10-006 Cross-Site Request Forgery (CSRF) vulnerability in Scott Kingsley Clark Crony Cronjob Manager |  |  |  |
|  | VA-2024-10-10-007 Linux Malware “Perfctl” Exploits Vulnerabiliy (CVE-2023-33246) and Misconfigurations |  |  |  |
|  | TA-MAW-2024-10-10-08 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-APT-2024-10-10-006 SideCopy Malware C&C IP |  |  |  |
|  | TA-PHI-2024-10-10-005 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-10-11-008 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2024-10-11-006 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-10-11-003 RCRU64 Ransomware |  |  |  |
|  | TA-MAW-2024-10-15-009 Malicious IOCs |  |  |  |
|  | TA-MAW-2024-10-15-010 Malicious IOCs |  |  |  |
|  | TA-TAG-2024-10-15-002 Threat Actor FlaxTyphoon |  |  |  |
|  | VA-2024-10-16-009 Active Exploitation Of  Ivanti Cloud Service Appliance (CSA) Flaws By Nation State Adversary |  |  |  |
|  | TA-PHI-2024-10-16-007 Malicious Domains used by Threat Actors |  |  |  |