**Cyber Security Advisories**

**Date: 19 Apr 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | Adv/2024/Mar/035 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Mar/036 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Mar/037 Phishing Attack |  |  |  |
|  | Adv/2024/Apr/001 Threat Group TA866 aka Asylum Ambuscade |  |  |  |
|  | Adv/2024/Apr/002 Malicious IOCs |  |  |  |
|  | Adv/2024/Apr/003 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Apr/004 Stately Taurus aka Mustang Panda |  |  |  |
|  | Adv/2024/Apr/005 Phishing Attack |  |  |  |
|  | Adv/2024/Apr/006 Malicious IOCs |  |  |  |
|  | Adv/2024/Apr/007 Phishing Attack |  |  |  |
|  | Adv/2024/Apr/008 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Apr/009 Critical Vulnerabilities in multiple Products |  |  |  |
|  | Adv/2024/Apr/010 Kimusky Group Distributes Malware to Deploy Endoor Backdoor |  |  |  |
|  | Adv/2024/Apr/011 Phishing Attack |  |  |  |
|  | Adv/2024/Apr/012 Various Ransomware Variants Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Apr/013 Malicious IOCs |  |  |  |
|  | Adv/2024/Apr/014 Safeguard \*nix(Unix/Linux) System  from backdoor attacks |  |  |  |
|  | Adv/2024/Apr/015 Brute Force Attacks Targeting Multiple VPN Services |  |  |  |
|  | Adv/2024/Apr/017 Critical Vulnerabilities & Security Updates in multiple Products |  |  |  |
|  | Adv/2024/Apr/018 FalseFont Backdoor |  |  |  |
|  | Adv/2024/Apr/019 DinodasRAT Malware Targeting Linux Servers |  |  |  |
|  | Adv/2024/Apr/020 WarzoneRAT Malware |  |  |  |
|  | Adv/2024/Apr/021 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Apr/022 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Apr/023 Phishing Domains |  |  |  |
|  | Adv/2024/Apr/024 Malicious IOCs |  |  |  |
|  | Adv/2024/Apr/025 Critical Vulnerabilities in Siemens Products |  |  |  |
|  | Adv/2024/Apr/026 Ramnit Trojan |  |  |  |
|  | Adv/2024/Apr/027 CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway |  |  |  |
|  | Adv/2024/Apr/029 Critical Vulnerabilities & Security Updates in multiple Products |  |  |  |
|  | Adv/2024/Apr/030 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Apr/031 Weekly Mirai Activity Report |  |  |  |
|  | CMTX-I-395042024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P042024646 Cerber Ransomware |  |  |  |
|  | CMTX-P-6280420249 Redline Malware Alert |  |  |  |
|  | CMTX-P-7940420249 Ursnif Malware Alert |  |  |  |
|  | CMTX-P-1520420249 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-1760420249 Raccoon Malware Alert |  |  |  |
|  | CMTX-P-2770420249 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-8320420249 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-5500420249 Emotet Malware Alert |  |  |  |
|  | CMTX-P-9940420249 Amadey Malware Alert |  |  |  |
|  | CMTX-P-2100420249 Qbot Malware Alert |  |  |  |
|  | CMTX-I-338042024 Phishing domain impersonating MoD website |  |  |  |
|  | CMTX-P042024864 Critical PuTTY Vulnerability |  |  |  |
|  | CMTX-P042024215A Critical Zero day Vulnerability (CVE-2024-3400) Affecting Palo Alto Networks PAN-OS software |  |  |  |
|  | CMTX-P042024205 CVE-2024-27309: Critical Vulnerability Affecting Apache Kafka |  |  |  |
|  | CMTX-P042024028 REDLINE STEALER MALWARE |  |  |  |
|  | CMTX-P042024038 RACCOON MALWARE |  |  |  |
|  | CMTX-P042024195 A Critical Zero day Vulnerability (CVE-2024-3400) Affecting Palo Alto Networks PAN-OS software |  |  |  |
|  | CMTX-P042024965 PLUGX RAT ALERT 113 |  |  |  |
|  | CMTX-P042024915 SHADOWPAD Malware |  |  |  |
|  | CMTX-P042024185 Rhadamanthys Info Stealer Malware |  |  |  |
|  | CMTX-P042024175 A Critical Vulnerability( CVE-2024-3273) Affecting D-Link NAS devices |  |  |  |
|  | CMTX-P042024636 QuasarRAT Malware ALERT 49 |  |  |  |
|  | CMTX-I-196042024 Phishing Domains - APT36 campaign |  |  |  |
|  | CMTX-P042024165 Matanbuchus Malware |  |  |  |
|  | CMTX-P042024155 A Critical Vulnerability in Rust standard library |  |  |  |
|  | CMTX-P042024135 APT34 threat actor activity |  |  |  |
|  | CMTX-P042024125 IceRAT Malware |  |  |  |
|  | CMTX-P042024115 Nova Stealer |  |  |  |
|  | CMTX-P042024115 Rilide Stealer |  |  |  |
|  | CMTX-P042024095 VIETNAM BASED THREAT ACTOR CORALRAIDER |  |  |  |
|  | CMTX-P042024105 SectopRAT |  |  |  |
|  | CMTX-P042024955 PLUGX RAT ALERT 112 |  |  |  |
|  | CMTX-P042024905 SHADOWPAD Malware |  |  |  |
|  | CMTX-P042024626 QuasarRAT Malware ALERT 48 |  |  |  |
|  | CMTX-P042024065 UNAPIMON Malware |  |  |  |
|  | CMTX-P042024018 REDLINE STEALER MALWARE |  |  |  |
|  | CMTX-P042024055 Critical Vulnerability (CVE-2024-2879) Impacting LayerSlider WordPress Plugin |  |  |  |
|  | CMTX-P042024045 DinodasRAT Malware |  |  |  |
|  | CMTX-P042024805 SHADOWPAD Malware |  |  |  |
|  | CMTX-P042024945 PLUGX RAT ALERT 111 |  |  |  |
|  | CMTX-P042024626 QuasarRAT Malware ALERT 47 |  |  |  |
|  | CMTX-I-025042024 GavaRAT - APT36 campaign |  |  |  |
|  | CMTX-P0420240105 CVE-2024-3094: Critical Vulnerability Affecting XZ Utils Data Compression Library |  |  |  |
|  | CMTX-P042024025 Hacktivist Group: R00TK1T ISC |  |  |  |