**Cyber Security Advisories**

**Date: 31 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-P012025505 ACTIVE EXPLOITATION OF A ZERO DAY VULNERABILITY AFFECTING FORTINET's PRODUCTS |  |  |  |
|  | CMTX-P-012025805 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-012025705 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-VUL-0120257715 Prominent Vulnerability List |  |  |  |
|  | CMTX-I-808012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-344012025 APT36 campaign |  |  |  |
|  | CMTX-I-563012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-024012025 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-026012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-065012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-390012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-012025855 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-012025865 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-891012025 IOCs of China-based Malware Campaign |  |  |  |
|  | CMTX-P-012025478 Nnice Ransomware |  |  |  |
|  | CMTX-I-044012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-012025488 J-magic Malware Campaign |  |  |  |
|  | CMTX-P-012025498 Murdoc Botnet Campaign |  |  |  |
|  | CMTX-I-180012025 SideCopy- C&C of Malware Campaign |  |  |  |
|  | CMTX-I-765012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-680012025 Linux Malware C&C IP |  |  |  |
|  | CMTX-I-356012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-VUL-012025518  Prominent Vulnerability List |  |  |  |
|  | CMTX-I-975012025 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-634012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-375012025 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-201012025 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P-012025744 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-012025865 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | TA-MAW-2025-01-15-016 Racoon Stealer Malware |  |  |  |
|  | TA-MAW-2025-01-15-017 Emotet Malware |  |  |  |
|  | TA-MAW-2025-01-15-018 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2025-01-15-009 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-15-019 Amadey Malware |  |  |  |
|  | TA-RAN-2025-01-15-002 RA World Ransomware Targeting Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-003 Black Basta Ransomware Targeting Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-004 Black Hunt Ransomware Targeting Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-005 Lockbit 3.0 Ransomware Targeting Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-006  RansomEXX v2.0 Ransomware Targeting Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-008 Presence of  BianLian Ransomware observed in Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-007 Presence of  AvosLocker Ransomware observed in Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-009 Presence of  RansomHub Ransomware observed in Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-01-16-010 Presence of Unknown Ransomware Variant observed in Indian CyberSpace |  |  |  |
|  | TA-MAW-2025-01-16-020 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-RAN-2025-01-16-011 FunkSec Ransomware |  |  |  |
|  | TA-MAW-2025-01-16-021 Venom Spider |  |  |  |
|  | TA-RAN-2025-01-16-012 Cozy Bear (APT29) Ransomware |  |  |  |
|  | VA-2025-01-17-007 CVE - KB Correlation, Jan 2025 |  |  |  |
|  | TA-PHI-2025-01-17-010 Phishing Attack |  |  |  |
|  | TA-APT-2025-01-17-005 APT SideCopy |  |  |  |
|  | TA-APT-2025-01-17-004 APT MirrorFace aka Earth Kasha |  |  |  |
|  | TA-PHI-2025-01-17-011 Phishing Attack |  |  |  |
|  | VA-2025-01-17-008 Active Exploitation of a Zero Day Vulnerability Affecting Fortinet's Products |  |  |  |
|  | TA-APT-2025-01-20-006 APT36 campaign |  |  |  |
|  | TA-MAW-2025-01-20-022 Mirai Botnet Campaign Exploiting Zero-day Vulnerabilities in Industrial Routers, Home Routers, Digital Video Recorder (DVRs), and Smart Home Devices |  |  |  |
|  | TA-MAW-2025-01-20-021 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-01-20-012 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-01-20-008 Prominent Vulnerability List |  |  |  |
|  | VA-2025-01-21-009 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-APT-2025-01-21-007 CrimsonRAT-  APT36 Campaign |  |  |  |
|  | TA-MAW-2025-01-21-023 RedDelta |  |  |  |
|  | SA-2025-01-22-002 Cyber Security Alert for Republic Day Ceremony & Beating The Retreat Ceremony-2025 |  |  |  |
|  | TA-PHI-2025-01-22-013 Phishing Attack |  |  |  |
|  | TA-MAW-2025-01-22-024 Malicious IOCs |  |  |  |
|  | TA-MAW-2025-01-22-025 Gafgyt Malware |  |  |  |
|  | TA-RAN-2025-01-22-013 Termite Ransomware |  |  |  |
|  | TA-APT-2025-01-23-008 APT Gamaredon |  |  |  |
|  | TA-MAW-2025-01-23-026 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-01-23-014 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-23-027 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2025-01-23-028 Tools used by Threat Groups for Cyber Espionage Campaign |  |  |  |
|  | VA-2025-01-23-010 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-01-24-029 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-APT-2025-01-24-009 APT Star Blizzard |  |  |  |
|  | TA-PHI-2025-01-28-015 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-28-029 IOCs of Malware Campaign |  |  |  |
|  | TA-RAN-2025-01-28-014 Nnice Ransomware |  |  |  |
|  | TA-MAW-2025-01-28-030 J-magic Malware Campaign |  |  |  |
|  | TA-MAW-2025-01-28-031 Murdoc Botnet Campaign |  |  |  |
|  | TA-APT-2025-01-28-010 APT Salt Typhoon |  |  |  |
|  | TA-MAW-2025-01-29-032 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2025-01-29-033 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-01-29-016 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2025-01-29-034 Malicious IOCs |  |  |  |
|  | VA-2025-01-29-011 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-01-29-035 Linux Malware C&C IP |  |  |  |
|  | TA-APT-2025-01-30-011 APT SideCopy |  |  |  |
|  | TA-MAW-2025-01-30-036 Malware Delivery via Malicious Ads |  |  |  |
|  | TA-PHI-2025-01-30-017 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2025-01-30-012 CrimsonRAT-  APT36 Campaign |  |  |  |
|  | VA-2025-01-30-012 Prominent Vulnerability List |  |  |  |