**Cyber Security Advisories**

**Date: 12 February 2025**

1. **CMTX-I-455022025: Malicious Domains used by Threat Actors**

VE-2024-55591 is a critical authentication bypass vulnerability affecting FortiOS and FortiProxy systems, allowing remote attackers to gain super-admin privileges. It exploits an alternate path or channel vulnerability, enabling unauthorized access to firewall

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

> Implement Multi-Factor Authentication to add a layer of security.

- ----------------------< Malicious Domain>-----------------

portal2.passportindia.gov.inq.srmcheck.me

\*.inq.srmcheck.me

- ----------------------</Malicious Domain>-----------------

Network administrators may take required action against the above malicious domains.