भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
राष्ट्रीय संचार सुरक्षा केंद्र

सत्यमेव जयते

Government of India
Ministry of Communications
Department of Telecommunications
National Centre for Communication Security

Ltr no. NCCS/SAS/ITSAR-Amendments/2024-25/1 Dated at Bangalore, the 23.10.2024

Sub: Amendments to WiFi CPE ITSAR

Ref: WiFi CPE ITSAR No ITSAR402122401 (Name: NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs)

Since the publishing of first version of above referred WIFi CPE ITSAR during November, 2018, the configuration and deployment scenario of WIFi CPEs changed over a period of time. In order to make the above referred WiFi CPE ITSAR applicable to split configuration wherein, the WiFi CPE is split into two or more devices like Access Point (AP), Controller etc., the following amendments/additions are made to the above referred ITSAR. These amendments/additions will come into force with immediate effect.

A. Amendments to existing clauses:

1. Clause No. 1.1.3: Role-Based access control

CPE shall support Role-Based Access Control (RBAC) which provides at least two different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the network product shall support RBAC with minimum of 3 user roles, in particular, for OAM privilege management for network product Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface. The RBAC provision should also be extended for Wi-Fi end users (for user-based access restriction) and API users (for different privilege levels), as applicable.

2. Clause No. 1.2.2: Authentication Support - External

If CPE supports external authentication (for the Cyber- Cafe use-case scenario), the user authentication credentials should be protected and securely communicated if the authentication credentials are managed by external authentication servers.

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the user authentication credentials should be protected and securely communicated (between AP & External authentication server or Controller and Authentication Server as applicable) if the authentication credentials are managed by external authentication servers.

3. Clause No. 1.2.3: Protection against brute force and dictionary attacks

CPE shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts.

CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it may implement at least one of the following most commonly used protection measures:

(a) Increasing the delay (e.g., doubling) for each newly entered incorrect password.

(b) Blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.

(c) Using CAPTCHA to prevent automated attempts.

This feature to be enabled for login attempts for CPE and on authentication attempts on Wi- Fi access through SSID with PSK.

Note: WPA3 also shall also be part of the protection measures.

4. Clause No. 1.5.1: Audit Event Generation

CPE to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.
In case of WiFi CPE split into two or more devices like AP, Controller etc., the controller shall store all the log data (as mentioned above) and also upload to a log server in a secure manner.

5. Clause No. 1.6.1: Cryptographic Based Secure Communication

The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The data is protected against well know attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc., and NIST specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc.
Additionally, if APIs are supported then the communication between API Server & Client should be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

6. Clause No. 1.6.3: Cryptographic Algorithm selection for Wi-Fi Access

It shall support WPA2-PSK with AES-128 as default standard. Other internationally accepted encryption standards stronger like AES-192 etc., may also be made available with user choice selection. Weaker encryption options like WEP, WPS, TKIP etc., are not to be available for selection / configuration.
Additionally, WPA2 version should support PMF (Protected Management Frames). WPA2 should have built in KRACK (Key Reinstallation Attack) Mitigation. Also, all the ciphers used must be in compliance with Table1 of the latest document "Cryptographic Controls for

Indian Telecom Security Assurance Requirements (ITSAR)". All types of Wi Fi CPEs should also support WPA3 and WPA should not be supported.

B. New Clauses added:

1. *Clause No. 1.3.11: Restricting System Boot Source*

The network product can boot only from the memory devices intended for this purpose. The network product can only boot from memory devices intended for this purpose (e.g., not from external memory like USB key).

2. *Clause No. 1.6.10: Avoidance of Unspecified Wireless Access*

An undertaking shall be given as follows: "The Network product does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel."

Note: Network product supporting standard wireless technologies would also need to be tested for this requirement apart from wireless technology related tests.

3. *Clause No. 1.7.2: Traffic Separation*

The Network product shall support physical or logical separation of O&M and control plane traffic. See RFC 3871 [3] for further information.

4. *Clause No. 1.10.7: No automatic launch of removable media*

The Network product shall not automatically launch any application when removable media device such as CD, DVD, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

5. *Clause No. 1.11.14: Restricted file access*

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g., via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.

6. *Clause No. 1.12.7 Avoidance of OWASP Top 10 API Security Risks*

If API s are supported, WiFi system should be free from OWASP top 10 API Security risks as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.

This issues with the approval of Sr.DDG, NCCS

DIRECTOR (SAS-III)
NCCS, Bangalore