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

NCCS
Securing Networks

Ltr no. NCCS/SAS/ITSAR-Amendments/2024-25/2 Dated at Bangalore, the 24.10.2024

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 technology of WIFi CPEs changed over a period of time. The WiFi CPE is deployed in split configuration wherein the WiFi CPE is split into two or more devices like Access Point (AP), Controller etc. Also, in some cases, the WiFi CPE components are hosted in a cloud environment. In order to adopt the above referred WiFi CPE ITSAR for such technological changes, 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.

7. <u>Clause No. 1.12.5: Unused Physical *and logical* Interfaces Disabling</u>

The CPE shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces (including LAN ports) *and logical interfaces* which are not under use shall be disabled by configuration so that they remain inactive even in the event of a reboot.

B. New Clauses added:

1. *<u>Clause No. 1.3.11: Restricting System Boot Source</u>*

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).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.2]

2. *<u>Clause No. 1.6.10: Avoidance of Unspecified Wireless Access</u>*

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. *<u>Clause No. 1.7.2: Traffic Separation</u>*

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1]

4. *<u>Clause No. 1.10.7: No automatic launch of removable media</u>*

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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.3]

5. *<u>Clause No. 1.11.14: Restricted file access</u>*

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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

6. *<u>Clause No. 1.12.7: Avoidance of OWASP Top 10 API Security Risks</u>*

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.*

7. Clause No. 1.12.8: The client and authorization servers shall mutually authenticate

APIs shall only allow themselves to be accessed by authorized users. One solution for authorizing access is the use of OAuth2.0 with access token. The client shall authenticate the resource server and vice versa. Mutual authentication is done by the transport layer protection and is required.

[Reference: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T23, BP-P1]

8. Clause No. 1.12.9: Authentication of the Request Originator

Before accepting the token as valid, the resource server shall authenticate the originator of the request as the legitimate owner of the token. The token is bound to the subject through the subject Identifier, which ensures that the token has been provided for this consumer.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

9. Clause No. 1.12.10: Requirements for client credentials

a) The client credentials shall be stored in a secure and tamper-resistant location or stored encrypted with the key protected in a tamper-resistant location.

b) The client credentials shall not be included in the source code and software packages.

c) The client credentials shall be installed in the client in a secure way, eliminating any possibility of gaining access to these credentials during installation.

d) The client credentials shall be possible for the authorization server to revoke the client credentials.

[Reference: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

10. Clause No. 1.12.11: Access Token shall be signed

The access token shall be signed to detect manipulation of the token or production of fake tokens. Access tokens shall be secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS). It shall be possible to encrypt the content of the access token.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

11. Clause No. 1.12.12: Format of Access Token

The access token shall be defined in a standard format (SAML or JWT).

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

12. Clause No. 1.12.13: Access tokens shall have limited lifetimes

The access token shall include a claim for the expiration time (expiration).

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

13. *<u>Clause No. 1.12.14: Access tokens shall be restricted to a particular number of operations</u>*

There shall be a restriction on the number of operations that an access token can perform in order to mitigate the replay attack by a malicious client.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

14. *<u>Clause No. 1.12.15: Access token shall be bound to the intended resource server.</u>*

The access token shall include a claim for the NF Instance Id of the Service Producer (audience). By using token binding, a client can enforce the use of a specified external authentication mechanism with the token.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

15. *<u>Clause No. 1.12.16: Tokens shall be bound to the client ID</u>*

The access token shall include a claim for the NF Instance Id of the Service Consumer (subject) which is the "Client ID."

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

16. *<u>Clause No. 1.12.17: Token Revocation</u>*

Token Revocation shall be possible. Unbound tokens shall not be used under any circumstance. The authorization server shall provide a mechanism for token revocation. If not, the lifetime of the Access token shall be kept very short, or the access token shall be single use. If a scheme to bind access tokens to the underlying transport layer relies on non-standard extensions, and those extensions are not available, the system shall fail securely, preventing a bid-down attack.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

C. New Clauses added
(Applicable only for WiFi CPE or any of its components implemented as Virtual Network Function (VNF)/Container Network Function (CNF)):

1. *<u>Clause No. 1.13.1: VNF/CNF network security profile</u>*

a) Each VNF/CNF supporting VNFC functions shall have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections.

b) The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection. There shall never be a requirement for all ports to be open, particularly on external standard-based interfaces (e.g. GTP).

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

2. *<u>Clause No. 1.13.2: Protection from buffer overflows</u>*

The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.5]

3. Clause No. 1.13.3: Data at rest storage

All user related data removed from the data at rest and the storage shall be cleaned.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest]

Note: Cleaned here means overwrite storage by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

4. Clause No. 1.13.4: VNF/CNF Startup

VNF/CNF startup shall include a secure boot process.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.19]

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

5. Clause No. 1.13.5: Trusted Time Source

The VNF/CNF shall synchronize with trusted time source.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.20]

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

6. Clause No. 1.13.6: VNF/CNF integration with authentication and authorization services

The VNF/CNF shall integrate with the organization's authentication and authorization services, e.g., IDAM (Identity Access Management). Limiting the number of repeated failed login attempts (configurable) reduces the risk of unauthorized access via password guessing (Bruce force attack). The restriction on the number of consecutive failed login attempts ("lockout_failure_attempts") and any actions post such access attempts (such as locking the account where the "lockout duration" is left unspecified) shall abide by the organization's policies.

[Reference: 1) ONAP - VNF API security requirements, October 2022 2) GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0 section: 6.3.2.2]

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

7. Clause No. 1.13.7: VNF/CNF Host Spanning

a) All control plane data in transit between hosts shall be sent over an encrypted and authenticated channel using the protocols as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)."

b) User plane traffic between hosts should be protected.

c) The system shall prevent and detect unauthorized VNF/CNF host spanning.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.15]

8. Clause No. 1.13.8: Input validation

The VNF/CNF must implement the following input validation controls:

i) Size (length) of all input shall be checked.

ii) Large-size input that can cause the VNF/CNF to fail shall not be allowed. If the input is a file, the VNF /CNF API must enforce a size limit.

iii) Input that contains content or characters inappropriate to the input expected by the design shall not be permitted. Inappropriate input, such as SQL expressions shall not be allowed.

[Reference: ONAP- VNF API security requirements, October 2022]

9. Clause No. 1.13.9: Key Management and security within cloned images

Cloned images shall not possess cryptographic key pairs utilized by their original image. Propagation of two or more images with the same key pairs immediately cancels out the notion of utilizing key pairs for the purpose of establishing identity.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.1]

10. Clause No. 1.13.10: Encrypting VNF/CNF volume/swap areas

a) The VNF/CNF volumes shall be secured by encrypting them and storing the cryptographic keys at safe locations. TPM or HSM modules can be used to securely store these keys.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

b) VM or Container or container swap areas shall be encrypted.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T14]

11. Clause No. 1.13.11: Encrypted Data Processing

a) Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs/CNFs on trusted and well-known hosts.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

b) It shall be possible to further restrict VNFs/CNFs on a single host depending on whether they handle decrypted sensitive data.

c) These controls shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.

d) The system shall prevent and detect unauthorized data manipulation and leakage (e.g., modification of VNF/CNF images, instantiating parallel VM(s) on same physical CPU).

[Reference: 3GPP TR 33.848-0.11.0 Section 5.16]

12. Clause No. 1.13.12: GVNP Life Cycle Management Security

a) VNF shall authenticate VNFM when VNFM initiates a communication to VNF.

b) VNF shall be able to establish securely protected connection with the VNFM.

c) VNF shall check whether VNFM has been authorized when VNFM access VNF's API.

d) VNF shall log VNFM's management operations for auditing.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.1]

Note: This test case is optional when the VNF and VNFM belongs to the same VNF vendor. If the VNF and VNFM belongs to the same VNF vendor and the interface between VNF and VNFM is proprietary interface, the API level authorization is not needed

13. Clause No. 1.13.13: Instantiating VNF from trusted VNF image

A VNF shall be initiated from one or more trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the organization.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.3]

14. Clause No. 1.13.14: Inter-VNF and intra-VNF Traffic Separation

The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affecting each other.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.5.8.5.2]

15. Clause No. 1.13.15: Security functional requirements on virtualization resource management

a) To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, and the VNF shall alert the OAM when the VNF cannot detect a VNFC message.

b) A VNF shall log the access from the VIM.

[Reference: 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022)]

16. Clause No. 1.13.16: VNF package and VNF image integrity

1) VNF package and the image shall contain integrity validation value (e.g. MAC).

2) VNF package shall be integrity protected during on boarding.

[Reference: 3GPP TS 33.818- 17.1.0 Section 5.2.5.5.3.3.5.1 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

17. Clause No. 1.13.17: Proper image management of VM images must be done

Images shall be carefully protected against unauthorized access, modification, and replacement by both systems and human actors.

a) Small number of images must be kept.

b) Images must be kept updated to avoid known vulnerability exploits.

c) Cryptographic checksum protection must be used to detect unauthorized changes to images and snapshots.

d) Strict control around access, creation and deployment of images/instances must be implemented. Such activities must be recorded for audit purposes.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017) G-07, PG 37, OS-01, OS-02]

18. Clause No. 1.13.18: Secrets in NF Container/VM Image

The VNF/CNF images shall not be packaged with embedded secrets such as passwords or credentials, or any other critical configuration data.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.28]

Note: All the above amended/new clauses and the clauses mentioned in WiFi CPE ITSAR No. ITSAR40212240 shall be tested for all applicable component systems/interfaces including cloud hosted components/systems.

This issues with the approval of Sr.DDG, NCCS

Digitally signed by
Nampalli Janardhan
Date: 25-10-2024 10:52:05
DIRECTOR (SAS-II)
NCCS, Bangalore