(1)

Telecommunication Engineering Centre
(Department of Telecommunications)
Khurshid Lal Bhawan, Janpath, New Delhi - 110 001
https://www.tec.gov.in/

No. 5-2/2021-TC/TEC/131 Dated: 13/06/2022

Amendment Notification

Subject: Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) phase-III and IV products-reg.

Ref: No. 5-2/2021-TC/TEC/112 dated: 31/01/2022

In partial modification to this office notification dated 31/01/2022 referred above **(enclosed)**, w.r.t. the testing and certification of telecommunication equipment under Phase-III and Phase-IV of MTCTE regime, as provisioned in Indian Telegraph (Amendment) Rules 2017, the following amendments/modification are hereby notified with immediate effect as mentioned below:

a. Extension of date of mandatory certification of MTCTE phase-III and IV products by twelve months i.e. from 01.07.2022 to 01.07.2023

b. Extension of last date of acceptance of test reports issued by labs accredited by International Laboratory Accreditation Cooperation (ILAC) signatories from non-border sharing countries by twelve months for technical parameters only i.e. from 30.06.2022 to 30.06.2023 for the products which were initially given ILAC relaxation till 30.06.2022 vide above referred amendment dated 31.01.2022.

This notification shall be applicable for all the products mentioned in notification issued vide 5-2/2021-TC/TEC/112 dated: 31/01/2022 except for the products mentioned in Gazette notification issued vide S.O. 2372(E) dated 24/05/2022. Further, all other conditions, details mentioned in notification issued vide 5-2/2021-TC/TEC/112 dated: 31/01/2022 shall remain unchanged.

This issues with approval of the Competent Authority.

Encl.: As above.

13.06.2022

निदेशक (टी°सी°-IV)/Director (TC-IV)
दूरसंचार अभियांत्रिकी केंद्र/Telecom Engineering Centre
खुर्शीद लाल भवन , जनपथ/ Khurshid Lal Bhawan, Janpath

Indian Telecom Security Assurance RequirementsFor

Wi-Fi CPEs

Security Assurance Standards (SAS),

National Center for Communications Security, BengaluruDepartment of Telecom, Ministry of Communications Government of India

India's Telecom Security Requirements for Wi-Fi CPE Equipment

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies securityrequirements for WiFi Customer Premises Equipment (CPE). The WiFi CPEs are the equipment that are used or deployed at customer premises in telecom networks for providinginternet connectivity to end users.

The types of devices for which ITSAR is applicable are WiFi Routers, WiFi Modems, Broadband Modems with WiFi facility, Cable Modems with WiFi facility, FTTH ONTs withWiFi facility, and WiFi Data cards which provide WiFi facility with backend 2G / 3G / 4G connectivity.

The security requirements are drawn from national, international standards and best securitypractices for telecom networks. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 is the reference document on which the ITSAR is modelled. The security requirements are grouped into 12 sections based on the sub-areas, the WiFi CPE

devices seeking certification has to meet thesecurity requirements mentioned in this document.

Access and Authorization

Management Protocols Entity Mutual Authentication

The CPE shall communicate with authenticated management entities only. The protocols used for the CPE management shall support mutual authentication mechanisms, preferably with pre-shared key arrangements Or by equivalent entity mutual authentication mechanisms. This shallbe verified for all protocols used for CPE management. (This feature shall be supported on all WAN management interfaces).

Management Traffic Protection

All management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods can support traffic encryption using protocolssuch as HTTPS, SSHv2 or can be based on lower tunnelling protocols (IPsec VPN, TLS VPN, etc.).

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 theyare authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.

User Authentication - Local/Remote

Local/Remote access to the CPE for configuration and maintenance purposes shall be grantedonly to authenticated users or machines using at least one authentication attribute. This authentication attribute when combined with the user name shall enable unambiguous authentication and identification of the authorized user. No methods to exist providing authentication-bypass attacks to succeed under all combinations of interface / methods ofauthentication.

Remote Management Standards

The remote management mechanisms for CPE to be fully compliant with the remote management standards that the OEM chose to implement, example: TR-069 or any other relevant standards, Such mechanisms to include entity mutual authentication, encryption of themanagement traffic.

Remote Management Standards for Connected Devices,Additional Features

The remote management mechanisms for devices connected to CPE, Or for configuration of additional features of CPE like DDNS, UPnP etc., are to be compliant with the respective latest standards published at the time of commencement of security testing. These additional features are to be configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection. Such mechanisms to include entity mutual authentication, encryption of the management traffic.

Unambiguous identification of the user & group

The CPE shall identify each login user unambiguously. CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials, or sharing of the same account between several users shall not be enabled by CPE.

Authentication and Attribute Management

Authentication Policy

The usage of a system functions such as network services (like SSH, SFTP, Web services), management access, local usage of operating systems and applications shall be allowed only after successful authentication on the basis of the user identity and at least one authentication attribute (e.g. password, certificate).

This requirement shall also be applied to accounts that are only used for communication between systems.

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.

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.

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

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

Using CAPTCHA to prevent automated attempts .

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

Enforce Strong Password

CPE shall only accept passwords that comply with the following complexity criteria:

Password containing a minimum length of 8 characters are only permitted by default. shorterlengths shall be rejected by the NE.

Minimum password length - the default minimum value of 8 characters.

Password comprises at least three of the following categories:

at least 1 uppercase character (A-Z)

at least 1 lowercase character (a-z)

at least 1 digit (0-9)

at least 1 special character (e.g. @;!$.)

CPE shall support password field length of minimum 64 characters.

This Feature to be enabled for CPE Login-IDs as well as for the PSK key associated with SSIDfor Wi-Fi access.

Inactive Session Timeout

CPE shall monitor inactive sessions of administrative login users, Data users either on LAN or WiFi and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues fora defined period, Session /user ID time out must occur after this inactivity. The timer values canbe admin configurable as per requirement. When the time out occurs the same screen must be cleared of all displayed information.

Password Change facility, 1st Installation /Factory Reset

Cpe CPE shall enforce change of authentication attribute (eg:- password) on 1st installationconfiguration or On factory reset conditions. If a password is used as an authentication

attribute, then the CPE shall provide a function that facilitates the user to change his password at any time. However, the CPE shall not allow the previously used passwords up to a certain number (Password History).

Protected Authentication feedback

When a user enters the password at the local console, local or remote management GUI, the CPE should give obscure feedback by displaying characters like "*".

Removal of predefined or default authentication attributes

CPE may come with predefined (by the vendor, developer or producer) authentication attributes such as password or cryptographic keys. CPE shall remove the predefined / default authentication attributes from its run-time configuration. Such predefined authentication attributes can be restored only through factory reset, preferably through operating a physical button.

Storage of Passwords in encrypted form

User passwords should be stored using password hashes or encrypted, based on a strong hashing mechanism designed for use with passwords (example: HMAC, PBKDF2, Argon2), OEM may choose his own hashing mechanism for implementation. Passwords may not be stored in clear text. This requirement does not apply to pre-shared keys that must be used in raw form, such as IKE pre-shared keys.

Software Security

Secure Update

The update process should verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example:SHA2) for integrity before updating the software in the CPE. The update mechanism should prevent illegal software patching.

Secure Upgrade

CPE should support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity.

Source Code security assurance

Source code of the CPE (in high level programming language) shall be free from known security vulnerabilities , the high security critical weaknesses listed in the CWE database and all

the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10. OEM may provide Software Test Document (STD) in this regard.

Known Malware Check

The Operating System and the applications installed in the CPE shall be free from any known malware. The CPE shall support mechanism to carry out anti-malware checks. OEM to submit Software Test document (STD) to establish that the CPE is free from Known Malware.

No unused software

Unused software components or parts of software which are not needed for operation or functionality of the CPE shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data). OEM to provide Software Test Document (STD) in this regard.

Unnecessary Service Removal

The OEM to provide list of essential services and the related ports required for functioning of CPE, list of optimal services supported by CPE and their related ports. The CPE shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services and their ports shall be initially configured to be disabled on the CPE by the vendor.

FTP

TFTP

Telnet

rlogin, RCP, RSH

HTTP

SNMPv1 and v2

SSHv1, HNAP

TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)

Finger

BOOTP server

Discovery protocols (CDP, LLDP)

IP Identification Service (Identd)

PAD

MOP

Secure Time Synchronization

The CPE shall support time synchronization feature for its core functionality or for the additional supported functionality. For CPEs that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP.

The CPE clock shall be synchronized with NTP server in a secure manner. The CPE client should be able to verify the authentication and authorization of the NTP Server.

OEM shall plugin well known vulnerabilities, input validation vulnerabilities related to NTP feature.

Self-Testing

The CPE shall support the detection mechanism for identification of failure of underlying security mechanisms (such as software image integrity, runtime integrity, cryptographic modules etc) used. The CPE to perform such self-tests periodically/at the time of booting, visual indication on failure is a desirable feature.

Feature / Service Activation Policy

The CPE shall have factory default settings such that only the essential features / services and ports required for main operational needs of CPE are only enabled. Optional features, added services, futuristic service / applications are disabled by default. Such disabled services could only be enabled after successful authentication and selection by ADMIN user.

Restricted reachability of services

The CPE shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. OEM to map the essential services required to be accessed from WAN side, LAN side to limit access to services only on need / functionality basis. For Interfaces on which services are active, the reachability to be limited to legitimate communication peers. One such Use-case scenario is to restrict web-management access of CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.

System Secure Execution Environment

No unused functions

Unused functions of the CPEs' software and hardware shall be deactivated.

During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually, such functions shall be deactivated in the configuration of the CPE in permanent manner.

Also hardware functions which are not required for operation or function of the system (e.g. unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after CPE reboot.

OEM to provide report in this regard, List of the used functions of the CPE's software and hardware as given by the OEM shall match the list of used software and hardware functionsthat are necessary for the operation of the CPE.

No unsupported components

The CPE shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime. OEM to provide report and declaration to this effect.

No Known Vulnerabilities in System on Chip (SOC) solution

This test is applicable for such CPEs which have System on Chip solutions, where majority of CPE functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chip-vendor test report indicating that the SOC is free from malware, known-vulnerabilities.

User Audit

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.

Data Protection

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.

Cryptographic Based Secure Communication on Wi-FiAccess

The communication security dimension on WiFi access 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 security mechanism to protect against well known attacks like capture-decrypting, PIN detection, Key recovery, Key reinstallation attacks.

It shall support WPA2-PSK with AES as default standard. Other encryption options stronger than WPA2 may be made available under configuration menu for user choice selection.

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.

Crypto-Key Protection Mechanism

The CPE to have protection mechanisms against access to keys in the CPE against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroizng blocks of key etc.

Protecting data and information - Confidential SystemInternal Data

When CPE is not in debug (maintenance) mode, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).

Protecting data and information in storage

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.

Protection against Copy of Data

CPE shall have protection against creating a copy of data in use / data in transit. Protective measures should eixit against use of available system functions / software residing in CPE to create copy of data for illegal transmission. The software functions, components in the CPE for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

Protection against Data Exfiltration - Overt Channel

CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as FTP, HTTP, HTTPS IM, P2P, Email etc are to be forbidden if they are initiated by / originate from the CPE. Outbound-use of such services are to be disabled in the CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Protection against Data Exfiltration - Covert Channel

CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel,ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc are to be forbidden if they are initiated by / originate from the CPE. Outbound-use of such services are tobe disabled in the CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Network Services

Traffic Filtering - Network Level

The CPE shall provide a mechanism to filter incoming IP packets on any IP interface. It is preferable to configure Access Control List (ACL) as default deny-all on WAN port, with feature to enable the types of traffic permitted on user selection.

Attack Prevention Mechanism

Excessive Overload Protection

The CPE may provide security measures to deal with overload situations which may occur during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Filtering IP Options

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered. OEMs may refer to standards such as RFC 6192, RFC 7126.

Vulnerability Testing Requirements

Fuzzing - Network and Application Level

The protocols supported by the CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application level protocols supported by the equipment.

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, both in the OS and in the applications installed, that can be detected by.

Port Scanning

It shall be ensured that on all network interfaces, only vendor documented/identified ports on the transport layer respond to requests from outside the system.

List of the identified open ports shall match the list of network services that are necessary for the operation of the CPE.

SSID Scanning

The CPE shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It needs to provide disguised feedback to users on unsuccessful attempts without revealing of reason for failures. Option to hide / unhide SSID on user selection is an essential feature.

Indian Telecom Security Assurance RequirementsFor

IP Router

Security Assurance Standards (SAS),

National Center for Communications Security, BengaluruDepartment of Telecom, Ministry of Communications Government of India

Access and Authorization

Management Protocols Mutual Authentication

Requirement:

The protocols used for the Network Product's management shall support mutual authentication mechanisms.

There is mutual authentication of entities for management interfaces on the networkproduct.

HTTPS with TLS 1.2 , SNMP V3 Protocols are allowed

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1]

Management Traffic Protection

Requirement:

(a) Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard networkprotocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.Verify the mechanisms implemented to protect data and information in transferto and from the Network Product's OAM interface

Role-Based access control

Requirement:

The network product shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The domains could be Fault Management (FM), Performance Management (PM), System Admin, etc. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e. the specific operation command or command group (e.g. View, Modify, Execute).

The network product supports 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

User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse.To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.

Authentication attributes include:

Cryptographic keys

Token

Passwords

This means that authentication based on a parameter that can be spoofed (e.g. phone numbers, public IP addresses or VPN membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

NOTE: Several of the above options can be combined (dual-factor authentication) to achieve a higher level of security. Whether or not this is suitable and necessary depends on the protection needs of the individual system and its data and is evaluated for individual cases.

Remote login restrictions for privileged users

Requirement:

Direct login as root or equivalent highest privileged user shall be limited to the systemconsole only. Root user will not be allowed to login to the system remotely.

Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimumrequired for the tasks they have to perform.

Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating systemor of applications or that are generated by the same (e.g. configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

Unambiguous identification of the user & group accountsremoval

Requirement:

Users shall be identified unambiguously by the Router . Router shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. Router shall not enable the use of group accounts or group credentials, or sharing of the same account between several users, by default.

Authentication Attribute Management

Authentication Policy

Requirement:

The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operatingsystem and applications.

This requirement shall also be applied to accounts that are only used for communicationbetween systems. An exception to the authentication and authorization requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public.

Authentication Support – External

Requirement:

External authentication mechanism if supported by Network product (support authentication, authorisation and accounting server capabilities) should be throughsecure (encrypted) communication channel.

Protection against brute force and dictionary attacks

Requirement:

If a password is used as an authentication attribute, a protection against brute force and dictionary attacks that hinder password guessing shall be implemented. Brute force and dictionary attacks aim to use automated guessing to ascertain passwords for user and machine accounts. Various measures or a combination of these measures can be takento prevent this. The most commonly used protection measures are: (i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").(ii)Blocking an account following a specified number of incorrect attempts,.

However it has to be taken into account that this solution needs a process for unlockingand an attacker can force this to deactivate accounts and make them unusable. (iii)Using CAPTCHA to prevent automated attempts (often used for Web applications).

(iv) Using a password blacklist to prevent vulnerable passwords.

In order to achieve higher security, it is often meaningful to combine two or more of the measures named here. It is left to the vendor to select appropriate measures. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

NOTE 1: Password management and blacklist configuration may be done in a separate node that is different to the node under test, e.g. a SSO server or any other central credential manager.

Enforce Strong Password

Requirement:

(a) The setting by the vendor shall be such that a network product shall only accept passwords that comply with the following complexity criteria:

Absolute minimum length of 8 characters (shorter lengths shall be rejected by the network product). It shall not be possible setting this absolute minimum length to a lowervalue by configuration.

Comprising at least three of the following categories:

at least 1 uppercase character (A-Z)

at least 1 lowercase character (a-z)

at least 1 digit (0-9)

at least 1 special character (e.g. @;!$.)

The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The default minimum length is the value configured by the vendor before any operator-specific configuration has been applied. The special characters may be categorized in sets according to their Unicode category.

If a central system is used for user authentication password policy is performed on the central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause. If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Network Product.

When a user is changing a password or entering a new password the system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

Inactive Session Timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specifiedperiod of inactivity. It shall be possible to configure an inactivity time-out period.

NOTE: The kind of activity required to reset the timeout timer depends on the type of user session.

Password Changes

Requirement:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry.

Previously used passwords shall not be allowed up to a certain number (Password History).

The number of disallowed previously used passwords shall be:

Configurable;

Greater than 0;

And its default value shall be 3. This means that the Network product shall storeat least the three previously set passwords. The maximum number of passwords that the network product can store for each user is up to the manufacturer.

When a password is about to expire a password expiry notification shall be provided to the user. Above requirements shall be applicable for all passwords used(e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

This requirement shall be met either by Network product itself or in combination withexternal authentication system.

Protected Authentication feedback

Requirement:

(a) The Authentication attributes shall not be displayed in such a way that it could beseen and misused by a casual local observer. Typically, the individual characters of

the password are replaced by a character such as "*". Under certain circumstancesit may be permissible for an individual character to be displayed briefly during input. Such a function is used, for ex ample, on smartphones to make input easier.However, the entire password is never output to the display in plaintext.

Above requirements shall be applicable for all authentication attributes used(e.g. application-level,OS-level, etc.). An exception to this requirement is machine accounts

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it.

Software Security

Secure Update

Requirement:

Network product's system software updates should be secure and shall be based on signed certificates. Network product shall allow updates only if code signing certificate isvalid and time not expired, the software update integrity shall be verified by hashing mechanism (like SHA2).

Note : TSP's are responsible to ensure that Software updates/patches implemented aresecure and safe from any vulnerability. TSP's to maintain information about updates asper Licensing agreement /amendment conditions . However if there is any patch/update/version change which affects the security functionality then the details of the same should be reported to TTSC/DOT by vendor /TSP's

Secure Upgrade

Requirement:

Software package integrity shall be validated in the installation/upgrade stage.

Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keysor certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.

Tampered software shall not be executed or installed if integrity check fails.

A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2

Source code security assurance

Requirement:

Vendor shall ensure the following while developing Network product's OS /Application Software

Industry standard best practices of secure coding during the entire software development life cycle of the Network product Software,which includes vendor developed code, third party software and open source code libraries used/embedded inthe Network product

The Network product software is free from known security vulnerabilities, security weaknesses listed in the CWE database and all the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10

The binary file for Network product application is generated from the source code that is free from all the stated coding security vulnerabilities stated in (ii) Vendor shall submit Software Test Document (STD) to lab for scrutiny

Known Malware Check

Requirement:

Vendor shall submit Software Test Document (STD) of the network product proving that the network product is free from known malware/spyware to lab for scrutiny

No unused software

Requirement:

Unused software components or parts of software which are not needed for operation or functionality of the Network product shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data).

Unnecessary Service Removal

Requirement:

The Network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on the Network product by the vendor.

FTP

TFTP

Telnet

rlogin, RCP, RSH

HTTP

SNMPv1 and v2

SSHv1

TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)

Finger

BOOTP server

Discovery protocols (CDP, LLDP)

IP Identification Service (Identd)

PAD

MOP

As an alternative to disabling the HTTP service, it is also possible for this service to remain active for reasons of user friendliness. In this case, however, queries to the web service may not be answered directly on this port but from a redirected to HTTPS service.

NOTE 2: Full documentation of required protocols and services of the Network productand their purpose needs to be provided by the vendor as prerequisite for the test case.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

Restricting System Boot Source

Requirement:

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]

Document Name	ITSAR for Mobility Management Entity (MME)		
Doc. No.	Version	Release date	Enforcement date
ITSAR-IPR-0001	1.0	XX-XXX-XXXX	XX-XXX-XXXX

Secure Time Synchronization

Requirement:

Network Product shall provide reliable time and date information provided manually by itself or through NTP server. Network product should generates audit logs for all changes to time settings. Network product should support to configure authentication between itself and external NTP server

---

Self Testing

Requirement:

Network product shall perform self-tests to identify failures in its security Mechanisms during i)power on ii) when Administrator Instructs. (eg., integrity of thefirmware and software as well as for the correct operation of cryptographic functions,etc.,)

Restricted reachability of services

Requirement:

The network product shall restrict the reachability of services so that they can only bereached on interfaces where their usage is required. On interfaces were services areactive, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the network product itself.

EXAMPLE: Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted tointerfaces in the management network to support separation of management traffic fromuser traffic.

Avoidance of Unspecified Wireless Access

Requirement:

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.

Procedure for Security Certification of Telecommunication Equipment

INTRODUCTION

The Indian Telegraph Rules, 1951, PART XI, Testing & Certification of Telegraph, (Rule 528 to 537) provides that every Telecom equipment must undergo prior mandatory testing and certification.

In this context, Department of Telecommunications has come out with a "Communication Security Certification Scheme" vide document No. NCCS/ComSec/01/30032020 for Security Certification of Telecom equipment.

This subordinate document gives the detailed procedure for security testing and certification of Telecom equipment.

Any Original Equipment Manufacturer (OEM)/importer/dealer/Service Providers who wishes to sell or import, or use any Telecom equipment in India, shall have to obtain SecurityCertificate from National Centre for Communication Security (NCCS).

Certification process endeavors to ensure that Telecom equipment complies with the essential country specific Telecom security standards and requirements namely the Indian Telecom Security Assurance Requirements (ITSAR).

DEFINITIONS

All the definitions in the "Communication Security Certification Scheme" document shall be applicable for this document.

‘Authorized Indian representative (AIR)’ means a company or firm incorporated inIndia, which, in case of imported equipment, has been duly authorized by Foreign OEM tocarry out all obligations required under MTCTE in respect of the imported equipment.

‘BoM’ means Bill of Material, and is a file containing details of all major modules/ components of the model being offered for testing. In case of application for certification ofmultiple models, the BoM shall include such details of all models.

SCOPE OF CERTIFICATION

The scope of Security certification would cover all types of Telecom equipment to be soldin India or to be connected to Indian Telecom network for which ITSAR is available and in force.

The effective dates for certification becoming mandatory for different Telecom equipmentshall be notified by the Government separately.

The use of certified equipment, unless specifically exempted, shall be governed by extant guidelines and rules.

If the equipment is being imported for Research and Development or for demonstration purpose in India or as a sample for mandatory testing, prior security certification may be exempted for limited numbers of equipment.

Any uncertified equipment, which is not prohibited in India by any law, personally accompanied on inward foreign travel to India for personal use, may be exempted from mandatory testing and certification on self-declaration.

Security Testing under this scheme shall be done only in designated TSTLs. List of Designated TSTLs and their scope of testing are available in MTCTE portal

GENERAL

Any OEM/importer/dealer/user of Telecom equipment must first ensure that the model ofequipment he intends to sell or use is certified under this Scheme.

Certification needs to be obtained only once for one ‘model’ of equipment, and is applicablefor any quantity of the certified model of the equipment. A different model of the equipment needs separate certification.

The model with full configuration of hardware, interfaces and software is called the Main model. Associated models for the purpose of Security certification are those models which have identical software but having hardware which is a subset of the main model. Associatedmodels of the telecom equipment shall be certified without testing.

Only complete-in-itself, standalone, independent equipment are tested and certified under the scheme. Equipment modules/ components are not covered by the scheme. Further, combinations of independent equipment made to form systems are not certified under this scheme; instead, each independent equipment would need separate certification.

The Certificate shall be valid for five years from the date of issue.

NCCS may suspend/cancel the certificate, if it comes to the knowledge of NCCS of any violation of the extant guidelines and rules.

NCCS may issue such directions to OEMs/importers/dealers/users consistent with the Act, Rule or this procedure, as may be necessary, for smooth functioning of certification process.

The security certification procedures, which are detailed in this document, are subject to revision from time to time.

CERTIFICATION PROCESS

Security Certification process broadly consists of two parts; firstly, testing against applicable ITSAR, and secondly evaluation of test results for ensuring conformance with theserequirements. If equipment is found compliant with all applicable ITSAR, it will be certified to that effect.

Any applicant seeking certification under this scheme may apply online on MTCTE portal (https://www.mtcte.tec.gov.in).The applicant may provide relevant documents like (i) CompanyRegistration (ii) Letter issued by company authorizing him for related responsibilities. Additionally, in case of foreign OEMs, the applicant from Indian company shall provide documents in support of (iii) MoU between foreign OEM and Indian representative (AIR) for sale and support of the product in India, and (iv) authorizing the AIR for MTCTE related responsibilities.

The documents shall be scrutinized and any shortcoming in documents shall be intimated to the applicant. After rectification of shortcomings, applicant's registration shall be approved,after which he may submit application for testing/ certification.

Applicant shall select product to be certified, its variant details, available interfaces and associated models' information, if applicable, and shall upload Bill of Materials (BoM) file on the portal. BoM for the purpose of security certification shall include Software version of the Operating System, Database, Cryptography module and any other third party/proprietary software used in the equipment apart from other hardware details. After submission of his application the applicable ITSAR and the fee to be paid will be intimated/shown to the Applicant.

After payment of applicable fee, the applicant has to get his equipment tested against applicable ITSAR from any of the designated TSTL. TSTL is required to complete testing within a period of 16 weeks which includes any time required by the applicant to make good any non-compliance brought out during the testing.

NCCS may appoint a validator for technical oversight of the testing carried out in the TSTL.

After completion of testing the TSTL shall upload the Test reports along with signature of the tested equipment. Hard copy of the comprehensive test reports shall also be made over to NCCS unit. The Test reports shall be evaluated for compliance against applicable ITSAR by NCCS.

If equipment is found compliant with applicable ITSAR(s), a Certificate shall be issued to the applicant, for the specific model of equipment.

The certificate will normally be issued within 4-8 weeks from the date of submission of complete test results, depending upon complexity of equipment.

If ITSAR is amended and a new version of the ITSAR released, it will be applicable from a prospective date indicated in the new version of ITSAR. Until that time, existing ITSAR will be applicable.

Telecommunication Engineering Centre (TEC) or any other entity specified may be contacted for clarifications pertaining to application process.

FEES PAYABLE

The Fees charged under the Scheme will consist of Security Test Report Evaluation Feeas given below. This shall be payable over and above the fee prescribed by TEC as per Schedule of fees given in the latest version TEC MTCTE document “Testing and Certification Procedure”:

Group of equipment	Security Test Report Evaluation Fee ₹
A and B	2,00,000
C	2,50,000
D	3,50,000

The Security Test Report Evaluation Fee given above shall also be applicable for Certification modification involving security testing.

Renewal Fee is applicable, if application for renewal of certificate is made, and no testingor report evaluation is involved. The amount of this fee is same as Administrative fee, for the respective product group.

Fee for issue of temporary certificate will be same as renewal fee as prescribed under para 6.3.

Fees for contravention will be levied as prescribed in the Indian Telegraph (Amendment) Rules, 2017.

Testing Fee: Fees charged by TSTLs for conducting security testing shall be payable directly to the TSTL without involvement of MTCTE portal.

All fees are non-refundable.

The fees are to be deposited during the application process on MTCTE portal. During processing, the MTCTE portal will lead the user to the Non-Tax Revenue Portal (NTRP) for online payment.

CERTIFICATE MODIFICATION

In the event of Software patch/ bug fix/ update, the certificate holder is responsible for ascertaining the compliance of certified equipment, including deployed equipment, with ITSAR

and apply for certificate modification. Whenever a patch/ bug fix/ update is released by OEM,it may be permitted to be deployed with a temporary certificate. OEM will submit the changedsignature along with all the internal test reports demonstrating to compliance to all security requirements of applicable ITSAR along with an undertaking given in the Annexure. The modified signature of the said model will be incorporated in a temporary certificate with a validity period of upto one year from the date of release or for balance period of initial certificatewhichever is earlier. Temporary certificate will be issued within 7 working days of Application normally. Any subsequent request for modification of temporary certificate will be allowed witha validity for balance period of that certificate.

In the event of Software patch/ bug fix/ update affecting any Security Functionality, recertification will be necessary subject to clause 7.3.

Modifications that can be differentiated as incremental change shall be permitted to undergo incremental testing.

Any modification in the certified product without a valid certificate shall amount to use of uncertified equipment and shall be dealt accordingly.

For renewal, a Certificate holder must apply online and pay the renewal fee at least one month prior to expiry of the current certificate's validity period.

A certificate shall be renewed only if there is no change in the ITSAR applicable to the equipment, and there is no change in the equipment model.

After evaluation of the renewal application, a fresh certificate valid for another five years shall be issued, indicating the previous certificate number thereon.

REVISION OF ITSAR

Technological developments, Country specific requirements, changes in international standards or other regulatory requirements may entail revision of ITSAR.

A new version of ITSAR will generally be issued along with a prospective date of effect indicated thereon.

The revision of ITSAR shall not generally affect the validity of certificate of already certifiedTelecom Equipment till the notified date of effect of new version of the ITSAR after which the equipment is to be certified against the new version of the ITSAR. The new version of ITSAR will indicate, for the equipment certified against the earlier version of ITSAR, whether the

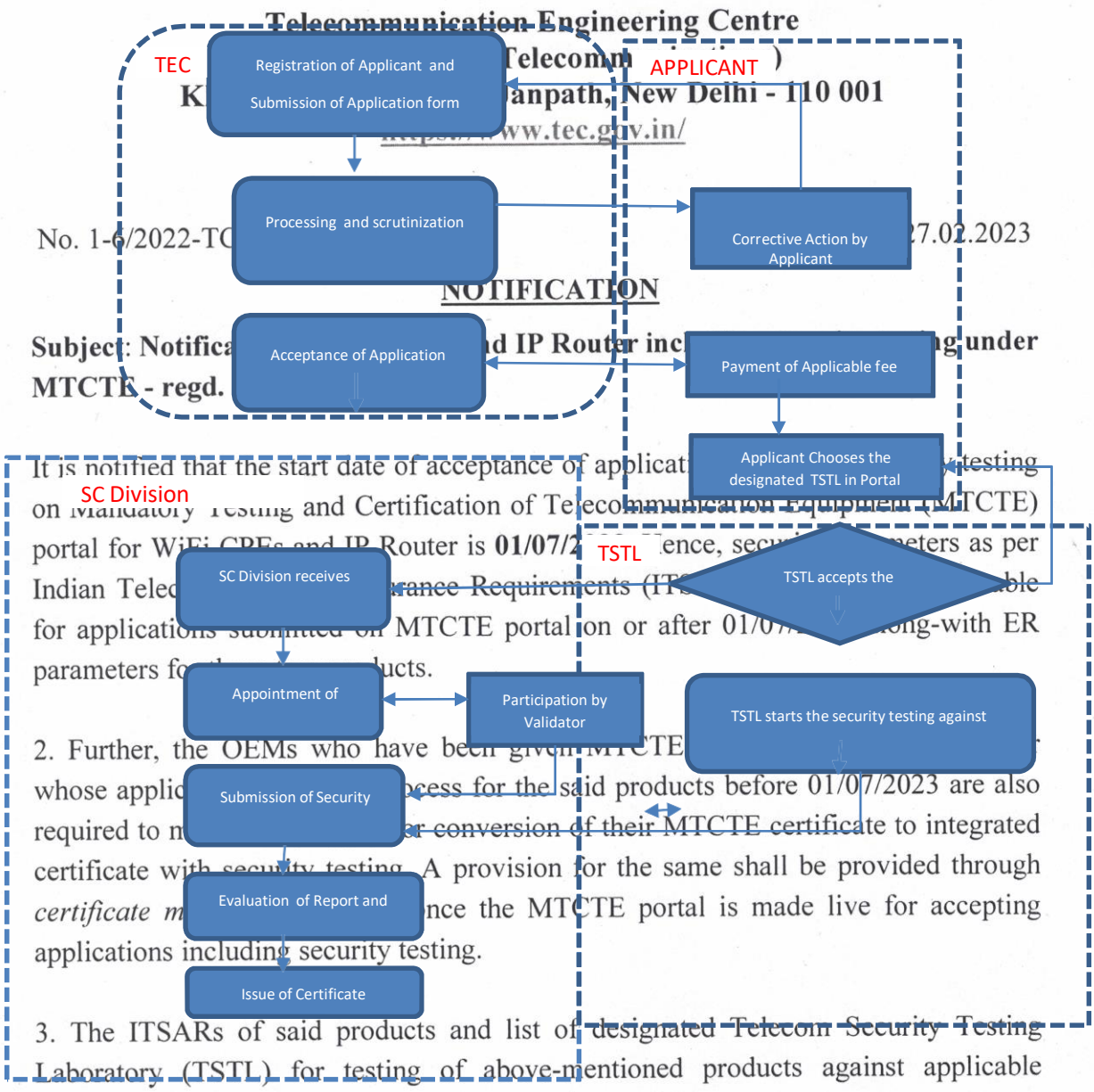
equipment requires to undergo full or incremental testing for certification against the new version of the ITSAR. Equipment for which applications are received after the notified date ofeffect of revised ITSAR shall be required to be certified against revised ITSAR. However, Government of India may direct the certificate holders to get specified models re-tested.

SURVEILLANCE

Appropriate Authority (AA) reserves the right to inspect and/ or test any telegraph, whichrequires mandatory certification at any time and at any premises including sites where it is in use or at the place of manufacturing to ensure that the telegraph used/ sold has required certifications and conforms to the ITSAR of existing certifications. Such inspection and/or testing may be carried out periodically, or at the discretion of Telegraph Authority or due to any complaint.

NCCS may call for re-testing/ re-evaluation of certified telecom equipment and charge the relevant fee, should the need arise to check on the compliance of the equipment to the ITSARs. These cases may be tested in Security Assurance Standards Facility of NCCS or designated TSTLs as decided by the Scheme Controller on a case-by-case basis.

Flow Chart for Security Certification



Telecommunication Engineering Centre

Telecomm) APPLICANT

K anpath, New Delhi - 110 001

ww.tec.gov.in/

No. 1-6/2022-TC 27.02.2023

NOTIFICATION

Subject: Notifica d IP Router inc g under MTCTE - regd.

It is notified that the start date of acceptance of applicat testing on Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) portal for WiFi CPEs and IP Router is **01/07/2** ence, secu eters as per Indian Telec rance Requirements (IT ble for applications submitted on MTCTE portal on or after 01/07/ long-with ER parameters fo ucts.

2. Further, the OEMs who have been given MTCTE whose applic cess for the said products before 01/07/2023 are also required to m r conversion of their MTCTE certificate to integrated certificate with security testing. A provision for the same shall be provided through *certificate m* nce the MTCTE portal is made live for accepting applications including security testing.

3. The ITSARs of said products and list of designated Telecom Security Testing Laboratory (TSTL) for testing of above-mentioned products against applicable ITSARs is available at NCCS website (https://nccs.gov.in).

This issues with the approval of Competent Authority.

22/02/2023

(Avadhesh Singh)
Director (TC-I)
dirta.tec@gov.in

(5)

Copy (through email) to:

1. Sr. DDG NCCS, Bangalore for kind information.
2. AD (IT), TEC for uploading on TEC/MTCTE website.
3. Office copy

(1)

Thông báo sửa dổi

Kiểm tra và chứng nhận bắt buộc đối với sản phẩm Thiết bị viễn thông giai đoạn III và IV

Tham chiếu: Số 5 -2/2021 - TC/TEC/112 ngày 31/01/2021

Thông báo sửa đổi một phần của văn bản này được đề cập ngày 31/12/2022 (có tệp đính kèm)w.r.t việc thử nghiệm và chứng nhận thiết bị viễn thông theo Giai đoạn III và Giai đoạn IV của chế độ MTCTE, được quy định trong Quy tắc Điện báo (Sửa đổi) Ấn Độ

năm 2017, các sửa đổi/sửa đổi sau đây được thông báo có hiệu lực ngay lập tức như được đề cập dưới đây.

Gia hạn ngày chứng nhận bắt buộc đối với sản phẩm Giai đoạn III và Giai đoạn IV thêm mười hai tháng, tức là từ ngày 07/01/2023.

Ngày gia hạn cuối cùng chấp nhận các báo cáo thử nghiệm do các phòng thí nghiệm được các bên ký kết Hợp tác Chứng nhận Phòng thí nghiệm Quốc tế (ILAC) công nhận từ các quốc gia chung không biên giới gia hạn thêm 12 tháng đối với các thông số kỹ thuật, tức là từ ngày 30.06.2022 đến ngày 30.06.2023 đối với các sản phẩm ban đầu do ILAC được nới lỏng cho đến ngày 30.6.2022 như trên đã đề cập đến bản sửa đổi ngày 30.01.2022.

Thông báo này được áp dụng cho tất cả các sản phẩm nêu tại thông báo ban hành số 5-2/2021-TC/TEC/112 ngày: 30/1/2022 ngoại trừ các sản phẩm nêu trong thông báo Gazette ban hành S.O 2372(E) ngày 24/ 05/2022. Ngoài ra, tất cả các điều kiện, chi tiết khác nêu tại thông báo 5-2/2021-TC/TEC/112 ngày: 31/01/2022 không thay đổi.

Vấn đề này được sự chấp thuận của Cơ quan có thẩm quyền.

(2)

Yêu cầu đảm bảo an ninh viễn thông của Ấn Độ đối với thiết bị CPE Wi-Fi

Tài liệu Yêu cầu Đảm bảo An ninh Viễn thông (ITSAR) của Ấn Độ này nêu rõ các yêu cầu bảo mật đối với Thiết bị được đặt tại cơ sở khách hàng WiFi (CPE). CPE WiFi là thiết bị được sử dụng hoặc triển khai tại cơ sở của khách hàng trong mạng viễn thông để cung cấp kết nối Internet cho người dùng.

Các loại thiết bị mà ITSAR có thể áp dụng là Bộ định tuyến WiFi, Modem WiFi, Modem băng thông rộng có thiết bị WiFi, Modem cáp có thiết bị WiFi, FTTH ONT có thiết bị WiFi và Thẻ dữ liệu WiFi cung cấp thiết bị WiFi với kết nối 2G / 3G / 4G phụ trợ

Các yêu cầu bảo mật được tuân thủ theo các tiêu chuẩn quốc gia, quốc tế và các biện pháp bảo mật tốt nhất cho mạng viễn thông. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 là tài liệu tham khảo mà ITSAR được mô hình hóa trên đó. Các yêu cầu bảo mật được nhóm thành 12 phần dựa trên các lĩnh vực phụ, các thiết bị WiFi CPE muốn được chứng nhận phải đáp ứng các yêu cầu bảo mật được đề cập trong tài liệu này.

Truy cập và ủy quyền

Cách thức quản lý xác thực thực thể đa chiều

CPE sẽ chỉ liên lạc với các thực thể quản lý được xác thực. Các giao thức được sử dụng để quản lý CPE phải hỗ trợ các cơ chế xác thực lẫn nhau, tốt nhất là với các sắp xếp khóa chia sẻ trước hoặc bằng các cơ chế xác thực lẫn nhau của thực thể tương đương. Điều này phải được xác minh cho tất cả các giao thức được sử dụng để quản lý CPE. (Tính năng này sẽ được hỗ trợ trên tất cả các giao diện quản lý WAN).

Quản lý bảo vệ mạng lưới giao thông

Tất cả lưu lượng quản lý phải được bảo vệ bằng tính toàn vẹn và mã hóa. Các phiên không được bảo vệ sẽ không được chấp nhận. Các phương thức truy cập từ xa có thể hỗ trợ mã hóa lưu lượng bằng các giao thức như HTTPS, SSHv2 hoặc có thể dựa trên các giao thức đường hầm thấp hơn (IPsec VPN, TLS VPN, v.v.).

Điều khiển truy cập dựa trên cơ sở vai trò

CPE sẽ hỗ trợ kiểm soát truy cập dựa trên vai trò (RBAC) cung cấp ít nhất hai cấp độ truy cập hoặc miền khác nhau để đảm bảo rằng các cá nhân chỉ có thể thực hiện các hoạt động mà họ được ủy quyền. Hệ thống RBAC kiểm soát cách người dùng được phép truy cập vào các miền khác nhau và loại hoạt động nào.

Xác thực người dùng – Cục bộ/ Từ xa

Quyền truy cập cục bộ/từ xa vào CPE cho mục đích cấu hình và bảo trì chỉ được cấp cho người dùng hoặc máy được xác thực sử dụng ít nhất một thuộc tính xác thực. Thuộc tính xác thực này khi kết hợp với tên người dùng sẽ cho phép xác thực và nhận dạng rõ ràng người dùng được ủy quyền. Không có phương pháp nào tồn tại để cung cấp các cuộc tấn công bỏ qua xác thực thành công dưới mọi kết hợp giao diện/phương thức xác thực.

Tiêu chuẩn quản lý từ xa

Các cơ chế quản lý từ xa để CPE tuân thủ đầy đủ các tiêu chuẩn quản lý từ xa mà OEM đã chọn thực hiện, ví dụ: TR-069 hoặc bất kỳ tiêu chuẩn nào khác có liên quan, Các cơ chế đó bao gồm xác thực lẫn nhau của thực thể, mã hóa lưu lượng quản lý.

Tiêu chuẩn quản lý từ xa cho các thiết bị được kết nối, các tính năng bổ sung

Cơ chế quản lý từ xa cho các thiết bị được kết nối với CPE hoặc để định cấu hình các tính năng bổ sung của CPE như DDNS, UPnP, v.v., phải tuân thủ các tiêu chuẩn mới nhất tương ứng được công bố tại thời điểm bắt đầu kiểm tra bảo mật. Các tính năng bổ sung này phải được định cấu hình là bị tắt trong cài đặt mặc định của nhà sản xuất, với điều khoản cho phép người dùng bật các tính năng riêng lẻ khi chọn menu. Cơ chế như vậy bao gồm xác thực lẫn nhau của thực thể, mã hóa lưu lượng quản lý.

Nhận dạng rõ ràng người dùng và nhóm

CPE sẽ xác định rõ ràng từng người dùng đăng nhập. CPE sẽ có thể chỉ định các tài khoản cá nhân cho mỗi người dùng, trong đó người dùng có thể là một người hoặc đối với Tài khoản máy, một ứng dụng hoặc một hệ thống. Đó là một tính năng mong muốn để định cấu hình tên USERID ưa thích của người dùng trong menu cấu hình thay vì ID người dùng ADMIN được định cấu hình trước. CPE sẽ không cho phép CPE sử dụng tài khoản nhóm hoặc thông tin xác thực của nhóm hoặc chia sẻ cùng một tài khoản giữa nhiều người dùng.

Xác thực và quản lý thuộc ngữ

Chính sách xác thực

Việc sử dụng các chức năng hệ thống như dịch vụ mạng (như SSH, SFTP, dịch vụ Web), quyền truy cập quản lý, sử dụng cục bộ hệ điều hành và ứng dụng chỉ được phép sau khi xác thực thành công trên cơ sở danh tính người dùng và ít nhất một thuộc tính xác thực (ví dụ: mật khẩu, chứng chỉ).

Yêu cầu này cũng sẽ được áp dụng cho các tài khoản chỉ được sử dụng để liên lạc giữa các hệ thống.

Hỗ trợ xác thực - Bên ngoài

Nếu CPE hỗ trợ xác thực bên ngoài (đối với trường hợp sử dụng Cyber-cafe), thông tin xác thực người dùng sẽ được bảo vệ và truyền đạt an toàn nếu thông tin xác thực được quản lý bởi máy chủ xác thực bên ngoài.

Bảo vệ chống lại sự tấn công bạo lực và ngôn ngữ

CPE phải có cơ chế cung cấp khả năng bảo vệ chống lại các cuộc tấn công từ điển và lực lượng vũ phu nhằm mục đích sử dụng tính năng đoán thủ công/tự động để lấy mật khẩu cho tài khoản người dùng và máy.

CPE để phát hiện các nỗ lực đăng nhập không hợp lệ lặp đi lặp lại vào tài khoản bằng mật khẩu không chính xác trong một khoảng thời gian ngắn và nó có thể thực hiện ít nhất một trong các biện pháp bảo vệ được sử dụng phổ biến nhất sau đây

a) Tăng độ trễ (ví dụ: tăng gấp đôi) cho mỗi lần nhập sai mật khẩu mới.

b) Chặn một tài khoản sau một số lần thử sai nhất định (thường là 5) trong một khoảng thời gian nhất định.

c) Sử dụng CAPTCHA để ngăn chặn các nỗ lực tự động

Tính năng này sẽ được bật cho các lần đăng nhập CPE và các lần xác thực khi truy cập Wi-Fi thông qua SSID bằng PSK.

Thực hành bảo mật cao

CPE sẽ chỉ chấp nhận mật khẩu tuân thủ các tiêu chí phức tạp sau:

a) Mật khẩu có độ dài tối thiểu 8 ký tự chỉ được phép theo mặc định. độ dài ngắn hơn sẽ bị NE từ chối.

b) Độ dài mật khẩu tối thiểu - giá trị tối thiểu mặc định là 8 ký tự.

c) Mật khẩu bao gồm ít nhất ba trong số các loại sau:

- ít nhất 1 ký tự viết hoa (A-Z)

- ít nhất 1 ký tự chữ thường (a-z)

- ít nhất 1 chữ số (0-9)

- ít nhất 1 ký tự đặc biệt (ví dụ: @;!$.)

CPE sẽ hỗ trợ độ dài trường mật khẩu tối thiểu 64 ký tự.

Tính năng này sẽ được bật cho ID đăng nhập CPE cũng như khóa PSK được liên kết với SSID để truy cập Wi-Fi.

Hết phiên thời gian hoạt động

CPE sẽ giám sát các phiên không hoạt động của người dùng đăng nhập quản trị, người dùng dữ liệu trên mạng LAN hoặc WiFi và bắt đầu cơ chế khóa phiên dựa trên bộ hẹn giờ có thể định cấu hình của người dùng. Việc mở khóa phiên chỉ được phép bằng cách xác thực. Nếu khoảng thời gian không hoạt động tiếp tục kéo dài trong một khoảng thời gian xác định thì thời gian chờ của Phiên/ID người dùng phải xảy ra sau khi không hoạt động này. Các giá trị bộ hẹn giờ có thể được quản trị viên cấu hình theo yêu cầu. Khi hết thời gian chờ, tất cả thông tin hiển thị trên cùng một màn hình phải bị xóa.

Cơ sở thay đổi mật khẩu, cài đặt lần đầu / Khôi phục cài đặt gốc

CPE sẽ thực thi thay đổi tính năng xác thực (ví dụ: - mật khẩu) trên cấu hình cài đặt đầu tiên hoặc Trên các điều kiện khôi phục cài đặt gốc. Nếu mật khẩu được sử dụng làm thuộc tính xác thực thì CPE sẽ cung cấp chức năng tạo điều kiện cho người dùng thay đổi mật khẩu của mình bất kỳ lúc nào. Tuy nhiên, CPE sẽ không cho phép mật khẩu được sử dụng trước đó đạt đến một con số nhất định (Lịch sử mật khẩu).

Phản hồi về bảo vệ xác thực

Khi người dùng nhập mật khẩu vào bảng điều khiển cục bộ, GUI quản lý cục bộ hoặc từ xa, CPE sẽ đưa ra phản hồi khó hiểu bằng cách hiển thị các ký tự như “*”.

Loại bỏ các tính năng xác thực được xác định trước hoặc mặc định

CPE có thể đi kèm với các thuộc tính xác thực được xác định trước (bởi nhà cung cấp, nhà phát triển hoặc nhà sản xuất) như mật khẩu hoặc khóa mật mã. CPE sẽ loại bỏ các thuộc tính xác thực mặc định/được xác định trước khỏi cấu hình thời gian chạy của nó. Các thuộc tính xác thực được xác định trước như vậy chỉ có thể được khôi phục thông qua khôi phục cài đặt gốc, tốt nhất là thông qua thao tác bằng nút vật lý.

Lưu trữ mật khẩu ở dạng mã hóa

Mật khẩu người dùng phải được lưu trữ bằng mật khẩu hoặc mã hóa, dựa trên cơ chế băm mạnh được thiết kế để sử dụng với mật khẩu (ví dụ: HMAC, PBKDF2, Argon2), OEM có thể chọn cơ chế băm của riêng mình để triển khai. Mật khẩu có thể không được lưu trữ ở dạng văn bản rõ ràng. Yêu cầu này không áp dụng cho các khóa chia sẻ trước phải được sử dụng ở dạng thô, chẳng hạn như khóa chia sẻ trước IKE.

Phần mềm bảo vệ

Cập nhật an toàn

Quá trình cập nhật phải xác minh tính xác thực của kho lưu trữ nguồn và tính toàn vẹn của bản vá phần mềm, tốt nhất là sử dụng Chứng chỉ kỹ thuật số để xác thực và băm (ví dụ: SHA2) để đảm bảo tính toàn vẹn trước khi cập nhật phần mềm trong CPE. Cơ chế cập nhật sẽ ngăn chặn việc vá phần mềm bất hợp pháp.

Nâng cấp an toàn

CPE phải hỗ trợ kiểm tra tính xác thực và tính toàn vẹn trong khi thực hiện nâng cấp phần mềm. Tốt nhất nên sử dụng Chứng chỉ kỹ thuật số để xác thực và băm (ví dụ: SHA2) để đảm bảo tính toàn vẹn.

Đảm bảo an toàn mã nguồn

Mã nguồn của CPE (bằng ngôn ngữ lập trình cấp cao) sẽ không có các lỗ hổng bảo mật đã biết, các điểm yếu nghiêm trọng về bảo mật cao được liệt kê trong cơ sở dữ liệu CWE và tất cả các lỗ hổng bảo mật có thể khai thác được liệt kê trong SANS Top 25 và OWASP Top 10 mới nhất. OEM có thể cung cấp Tài liệu Kiểm thử Phần mềm (STD) về vấn đề này.

Kiểm tra phần mềm độc hại

Hệ điều hành và các ứng dụng được cài đặt trong CPE sẽ không có bất kỳ phần mềm độc hại nào đã biết. CPE phải hỗ trợ cơ chế thực hiện kiểm tra chống phần mềm độc hại. OEM gửi tài liệu Kiểm tra phần mềm (STD) để chứng minh rằng CPE không có Phần mềm độc hại trước đó.

Không tồn tại các phần mềm không cần thiết

Các thành phần phần mềm không sử dụng hoặc các bộ phận của phần mềm không cần thiết cho hoạt động hoặc chức năng của CPE sẽ không được cài đặt hoặc sẽ bị xóa sau khi cài đặt. Điều này cũng bao gồm các phần của phần mềm, sẽ được cài đặt làm ví dụ nhưng thường không được sử dụng (ví dụ: các trang web mặc định, cơ sở dữ liệu mẫu, dữ liệu thử nghiệm). OEM cung cấp Tài liệu Kiểm tra Phần mềm (STD) về vấn đề này.

Loại bỏ dịch vụ không cần thiết

OEM cung cấp danh sách các dịch vụ thiết yếu và các cổng liên quan cần thiết cho hoạt động của CPE, danh sách các dịch vụ tối ưu được CPE hỗ trợ và các cổng liên quan của chúng. CPE sẽ chỉ chạy các trình xử lý giao thức và các dịch vụ cần thiết cho hoạt động của nó và không có bất kỳ lỗ hổng bảo mật nào đã biết. Cụ thể, theo mặc định, các dịch vụ sau và cổng của chúng sẽ được nhà cung cấp cấu hình ban đầu để vô hiệu hóa trên CPE.

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 và v2
- SSHv1, HNAP
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD

- MOP

Đồng bộ hóa an toàn thời gian

CPE phải hỗ trợ tính năng đồng bộ hóa thời gian cho chức năng cốt lõi của nó hoặc cho chức năng được hỗ trợ bổ sung. Đối với các CPE có tính năng đồng bộ hóa thời gian, nó sẽ hỗ trợ tính năng đồng bộ hóa thời gian an toàn tốt nhất bằng cách sử dụng Giao thức thời gian mạng NTP.

Đồng hồ CPE phải được đồng bộ hóa với máy chủ NTP một cách an toàn. Máy khách CPE sẽ có thể xác minh xác thực và ủy quyền của Máy chủ NTP.

OEM sẽ bổ sung các lỗ hổng đã biết, lỗ hổng xác thực đầu vào liên quan đến tính năng NTP.

Tự kiểm tra

CPE phải hỗ trợ cơ chế phát hiện để xác định lỗi của các cơ chế bảo mật cơ bản (như tính toàn vẹn hình ảnh phần mềm, tính toàn vẹn thời gian chạy, mô-đun mật mã, v.v.) được sử dụng. CPE thực hiện các hoạt động tự kiểm tra định kỳ/tại thời điểm khởi động, chỉ báo trực quan về lỗi là một tính năng đáng mong đợi.

Chính sách kích hoạt tính năng/dịch vụ

CPE phải cài đặt mặc định của nhà sản xuất sao cho chỉ các tính năng/dịch vụ và cổng thiết yếu cần thiết cho nhu cầu vận hành chính của CPE mới được bật. Tùy chọn tính năng, dịch vụ bổ sung, dịch vụ/ứng dụng tương lai bị tắt theo mặc định. Các dịch vụ được vô hiệu hóa chỉ có thể được bật sau khi người dùng ADMIN xác thực và lựa chọn thành công.

Khả năng tiếp cận dịch vụ bị hạn chế

CPE sẽ hạn chế khả năng tiếp cận của các dịch vụ để chúng chỉ có thể tiếp cận được trên các giao diện nơi việc sử dụng chúng được yêu cầu. OEM lập bản đồ các dịch vụ thiết yếu cần được truy cập từ phía WAN, phía LAN để hạn chế quyền truy cập vào các dịch vụ chỉ trên cơ sở nhu cầu/chức năng. Đối với các Giao diện có dịch vụ đang hoạt động, khả năng tiếp cận bị giới hạn ở các giao tiếp ngang hàng hợp pháp. Một kịch bản Ca sử dụng như vậy là hạn chế quyền truy cập quản lý web của CPE chỉ vào các cổng LAN và không cho phép truy cập trên Wi-Fi, phía WAN.

Môi trường thực thi hệ thống an toàn

Không có chức năng không sử dụng

Các chức năng không sử dụng của phần mềm và phần cứng của CPE sẽ bị vô hiệu hóa.

Trong quá trình cài đặt phần mềm và phần cứng, các chức năng thường sẽ được kích hoạt không cần thiết cho hoạt động hoặc chức năng của hệ thống. Nếu không thể xóa hoặc gỡ cài đặt riêng các chức năng không sử dụng của phần mềm thì các chức năng đó sẽ bị vô hiệu hóa vĩnh viễn trong cấu hình của CPE.

Ngoài ra, các chức năng phần cứng không cần thiết cho hoạt động hoặc chức năng của hệ thống (ví dụ: các giao diện không được sử dụng) sẽ bị vô hiệu hóa vĩnh viễn. Vĩnh viễn có nghĩa là chúng sẽ không được kích hoạt lại sau khi khởi động lại CPE.

OEM cung cấp báo cáo về vấn đề này. Danh sách các chức năng được sử dụng của phần mềm và phần cứng của CPE do OEM cung cấp phải khớp với danh sách các chức năng phần mềm và phần cứng được sử dụng cần thiết cho hoạt động của CPE.

Không có thành phần không được hỗ trợ

CPE không chứa các thành phần phần mềm và phần cứng không còn được nhà cung cấp, nhà sản xuất hoặc nhà phát triển của họ hỗ trợ, chẳng hạn như các thành phần đã hết vòng đời hoặc hết hỗ trợ. Không bao gồm các thành phần có hợp đồng hỗ trợ đặc biệt. Hợp đồng này sẽ đảm bảo việc khắc phục các lỗ hổng trong suốt vòng đời của các thành phần. OEM để cung cấp báo cáo và tuyên bố về hiệu ứng này.

Không có lỗ hổng trong giải pháp Hệ thống trên Chip (SOC)

Thử nghiệm này có thể áp dụng cho các CPE có giải pháp Hệ thống trên Chip, trong đó phần lớn các chức năng CPE được thực hiện trong chip VLSI. OEM cung cấp báo cáo thử nghiệm tự kiểm tra/bên thứ ba/nhà cung cấp chip cho biết rằng SOC không có phần mềm độc hại, các lỗ hổng đã biết.

Kiểm tra người dùng

Kiểm tra việc tạo sự kiện

CPE có khả năng ghi lại các sự kiện Bảo mật quan trọng. Nhật ký kiểm tra tốt nhất có thể được lưu trữ trong bộ nhớ ổn định. Nếu có thể áp dụng (đối với cyber-cafe, kịch bản sử dụng Văn phòng Dữ liệu Công cộng) thì phải tồn tại điều khoản về xuất nhật ký an toàn và nhật ký có thể ghi lại Tham chiếu Hệ thống duy nhất như địa chỉ trang web, Địa chỉ IP, địa chỉ MAC, tên máy chủ, số lần đăng nhập, v.v.

Bảo toàn dữ liệu

Truyền thông an toàn dựa trên mật mã

Kích cỡ truyền thông bảo mật đảm bảo rằng thông tin chỉ truyền giữa các điểm cuối được ủy quyền (thông tin không bị chuyển hướng hoặc bị chặn khi truyền giữa các điểm

cuối này). Dữ liệu được bảo vệ có khả năng chống lại các cuộc tấn công nổi tiếng liên quan đến Đánh hơi, Tiết lộ, trinh sát, v.v.,

Cơ chế liên lạc an toàn giữa CPE và các thực thể được kết nối sẽ sử dụng các giao thức tiêu chuẩn ngành như IPSEC, VPN, SSH, TLS/SSL, v.v. và các thuật toán mã hóa do NIST chỉ định với các kích thước khóa cụ thể như SHA, Diffie-Hellman, AES, v.v.

Giao tiếp an toàn dựa trên mật mã khi truy cập Wi-Fi

Kích thước bảo mật liên lạc khi truy cập WiFi đảm bảo rằng thông tin chỉ truyền giữa các điểm cuối được ủy quyền (thông tin không bị chuyển hướng hoặc bị chặn khi truyền giữa các điểm cuối này). Cơ chế bảo mật để bảo vệ chống lại các cuộc tấn công phổ biến như bắt-giải mã, phát hiện mã PIN, Khôi phục khóa, tấn công cài đặt lại khóa.

Nó sẽ hỗ trợ WPA2-PSK với AES làm tiêu chuẩn mặc định. Các tùy chọn mã hóa khác mạnh hơn WPA2 có thể được cung cấp trong menu cấu hình để người dùng lựa chọn.

Lựa chọn thuật toán mã hóa để truy cập Wi-Fi

Nó sẽ hỗ trợ WPA2-PSK với AES-128 làm tiêu chuẩn mặc định. Các tiêu chuẩn mã hóa được quốc tế chấp nhận mạnh hơn như AES-192, v.v., cũng có thể được cung cấp theo lựa chọn của người dùng. Các tùy chọn mã hóa yếu hơn như WEP, WPS, TKIP, v.v., sẽ không có sẵn để lựa chọn / cấu hình.

Cơ chế bảo vệ khóa mật mã

CPE phải có các cơ chế bảo vệ chống lại việc truy cập vào các khóa trong CPE chống lại việc tiết lộ Khóa, trinh sát, tấn công cài đặt lại, không đặt lại, chặn khóa Zeroizng, v.v.

Bảo vệ dữ liệu, thông tin – Hệ thống bí mật của dữ liệu nội bộ

Khi CPE không ở chế độ gỡ lỗi (bảo trì), sẽ không có chức năng hệ thống nào tiết lộ rõ ràng dữ liệu nội bộ của hệ thống bí mật cho người dùng và quản trị viên. Các chức năng hệ thống như vậy có thể là, ví dụ: OAM CLI hoặc GUI cục bộ hoặc từ xa, thông báo lỗi, thông báo ghi nhật ký, cảnh báo, xuất tệp cấu hình, v.v. Dữ liệu nội bộ của hệ thống bí mật cũng chứa dữ liệu xác thực (ví dụ: mã PIN, khóa mật mã, mật khẩu, cookie) là dữ liệu nội bộ của hệ thống không cần thiết cho việc quản trị hệ thống và có thể mang lại lợi ích cho những kẻ tấn công (tức là ngăn xếp dấu vết trong thông báo lỗi).

Bảo vệ dữ liệu và kho lưu trữ thông tin

Đối với dữ liệu nhạy cảm trong bộ lưu trữ (liên tục hoặc tạm thời), quyền truy cập đọc sẽ bị hạn chế. Các tập tin của hệ thống cần thiết cho chức năng phải được bảo vệ khỏi sự thao túng.

Bảo vệ chống sao chép dữ liệu

CPE phải có biện pháp bảo vệ chống lại việc tạo bản sao dữ liệu đang được sử dụng/dữ liệu đang truyền. Các biện pháp bảo vệ nên ngăn chặn việc sử dụng các chức năng/phần mềm hệ thống có sẵn trong CPE để tạo bản sao dữ liệu nhằm mục đích truyền tải bất hợp pháp. Các chức năng, thành phần phần mềm trong CPE để tạo bản sao dữ liệu phải bị vô hiệu hóa hoặc được bảo mật đầy đủ để ngăn chặn việc sao chép dữ liệu bất hợp pháp.

Bảo vệ chống rò rỉ dữ liệu - Kênh công khai

CPE phải có cơ chế ngăn chặn các cuộc tấn công lấy cắp dữ liệu nhằm đánh cắp dữ liệu đang sử dụng/dữ liệu đang truyền. Việc thiết lập các kênh công khai gửi đi như FTP, HTTP, HTTPS IM, P2P, Email, v.v. đều bị cấm nếu chúng được khởi xướng/bắt nguồn từ CPE. Việc sử dụng ra bên ngoài các dịch vụ như vậy sẽ bị vô hiệu hóa trong CPE, nếu điều cần thiết là phải có một số dịch vụ này để sử dụng ra bên ngoài (quản lý từ xa, v.v.), thì phải tồn tại cơ sở để giám sát các kênh bất thường.

Bảo vệ chống đánh cắp dữ liệu - Kênh bí mật

CPE phải có cơ chế ngăn chặn các cuộc tấn công lấy cắp dữ liệu nhằm đánh cắp dữ liệu đang sử dụng/dữ liệu đang truyền. Việc thiết lập các kênh và đường hầm bí mật gửi đi như Đường hầm DNS, Đường hầm HTTPS, Đường hầm ICMP, TLS, SSL, SSH, IPSEC VPN, Đóng gói RTP, v.v. đều bị cấm nếu chúng được khởi tạo bởi/bắt nguồn từ CPE. Việc sử dụng ra bên ngoài các dịch vụ như vậy sẽ bị vô hiệu hóa trong CPE, nếu điều cần thiết là phải có một số dịch vụ này để sử dụng ra bên ngoài (quản lý từ xa, v.v.), thì phải tồn tại cơ sở để giám sát các kênh bất thường.

Dịch vụ mạng

Lọc lưu lượng - Cấp độ mạng

CPE sẽ cung cấp cơ chế lọc các gói IP đến trên bất kỳ giao diện IP nào. Tốt nhất nên định cấu hình Danh sách điều khiển truy cập (ACL) làm từ chối tất cả mặc định trên cổng WAN, với tính năng cho phép các loại lưu lượng được phép theo lựa chọn của người dùng.

Cơ chế ngăn tấn công

Bảo vệ các tình huống quá tải

CPE có thể cung cấp các biện pháp an ninh để giải quyết các tình huống quá tải có thể xảy ra trong thời gian lưu lượng truy cập tăng. Đặc biệt, phải tránh sự suy giảm một phần hoặc toàn bộ tính khả dụng của hệ thống.

Tùy chọn IP

Các gói IP có các tùy chọn hoặc tiêu đề mở rộng không cần thiết sẽ không được xử lý. Tùy chọn IP và tiêu đề mở rộng (ví dụ: định tuyến nguồn) chỉ được yêu cầu trong các trường hợp đặc biệt. Vì vậy, tất cả các gói có tùy chọn IP hoặc tiêu đề mở rộng được bật sẽ được lọc. OEM có thể tham khảo các tiêu chuẩn như RFC 6192, RFC 7126.

Yêu cầu kiểm tra lỗ hổng

Kiểm tra lỗi - Cấp độ mạng và ứng dụng

Các hình thức được CPE hỗ trợ phải mạnh khi nhận được đầu vào không mong muốn hoặc không đúng định dạng. Yêu cầu này phải được áp dụng cho cả giao thức cấp độ mạng cũng như cấp độ ứng dụng được thiết bị hỗ trợ.

Cổng quét

Phải đảm bảo rằng trên tất cả các giao diện mạng, chỉ các cổng được nhà cung cấp ghi lại/xác định trên lớp vận chuyển mới đáp ứng các yêu cầu từ bên ngoài hệ thống.

Danh sách các cổng mở được xác định phải khớp với danh sách các dịch vụ mạng cần thiết cho hoạt động của CPE.

Quét SSID

CPE không được tiết lộ thông tin nhạy cảm, chi tiết mã PIN về kỹ thuật quét/tấn công SSID. Nó cần cung cấp phản hồi được ngụy trang cho người dùng về những lần thử không thành công mà không tiết lộ lý do thất bại. Tùy chọn ẩn/hiện SSID theo lựa chọn của người dùng là một tính năng cần thiết.

(ví dụ QUAN TRỌNG, CHÍNH, NHỎ), loại kết quả (ví dụ: THÀNH CÔNG, THẤT BẠI).

(3)

Yêu cầu đảm bảo an ninh viễn thông Ấn Độ cho

Bộ định tuyến IP

Tiêu chuẩn đảm bảo an ninh (SAS),

Trung tâm An ninh Truyền thông Quốc gia, Cục Viễn thông Bengaluru, Bộ Truyền thông Chính phủ Ấn Độ

Truy cập và ủy quyền

Giao thức quản lý Xác thực lẫn nhau

Yêu cầu:

Các giao thức được sử dụng để quản lý Sản phẩm Mạng phải hỗ trợ các cơ chế xác thực lẫn nhau.

Có sự xác thực lẫn nhau của các thực thể cho các giao diện quản lý trên sản phẩm mạng.

Cho phép HTTPS với TLS 1.2, Giao thức SNMP V3

Quản lý bảo vệ

Yêu cầu:

Cần phải sử dụng các giao thức mạng được bảo vệ bằng mật mã. Việc truyền dữ liệu cần được bảo vệ phải sử dụng các giao thức mạng tiêu chuẩn của ngành với đầy đủ các biện pháp bảo mật và thuật toán được ngành chấp nhận. Cụ thể là phải sử dụng phiên bản giao thức không có lỗ hổng bảo mật hoặc giải pháp thay thế an toàn. Xác minh các cơ chế được triển khai để bảo vệ dữ liệu và thông tin khi truyền đến và đi từ giao diện OAM của Sản phẩm Mạng.

Điều khiển truy cập dựa trên cơ sở vai trò (điều khiển và đảm bảo quyền cho người sử dụng)

Yêu cầu:

Sản phẩm mạng phải hỗ trợ Kiểm soát truy cập dựa trên vai trò (RBAC). Hệ thống kiểm soát truy cập dựa trên vai trò sử dụng một bộ điều khiển xác định cách người dùng tương tác với miền và tài nguyên. Các miền có thể là Quản lý lỗi (FM), Quản lý hiệu suất (PM), Quản trị hệ thống, v.v. Hệ thống RBAC kiểm soát cách người dùng hoặc nhóm người dùng được phép truy cập vào các miền khác nhau và loại hoạt động nào họ có thể thực hiện, tức là cụ thể lệnh hoạt động hoặc nhóm lệnh (ví dụ: Xem, Sửa đổi, Thực thi).

Sản phẩm mạng hỗ trợ RBAC với tối thiểu 3 vai trò người dùng, đặc biệt là quản lý đặc quyền OAM để Quản lý và bảo trì sản phẩm mạng, bao gồm ủy quyền hoạt động cho dữ liệu cấu hình và phần mềm thông qua giao diện bảng điều khiển sản phẩm mạng

Xác thực người dùng (Cục bộ/ Từ xa)

Yêu cầu:

Các tài khoản người dùng và máy khác nhau trên hệ thống phải được bảo vệ khỏi việc lạm dụng. Để đạt được mục đích này, thuộc tính xác thực thường được sử dụng, khi kết hợp với tên người dùng, sẽ cho phép xác thực và nhận dạng rõ ràng người dùng được ủy quyền.

Các thuộc tính xác thực bao gồm:

- Khóa mật mã

- Mã thông báo

- Mật khẩu

Hạn chế đăng nhập từ xa đối với người dùng có đặc quyền

Đăng nhập trực tiếp với quyền root hoặc người dùng có đặc quyền cao nhất tương đương sẽ chỉ được giới hạn trong bảng điều khiển hệ thống. Người dùng root sẽ không được phép đăng nhập vào hệ thống từ xa.

Chính sách ủy quyền

Yêu cầu:

Việc ủy quyền cho các tài khoản và ứng dụng sẽ được giảm xuống mức tối thiểu cần thiết cho các nhiệm vụ mà chúng phải thực hiện.

Việc ủy quyền cho một hệ thống sẽ bị giới hạn ở mức độ mà người dùng chỉ có thể truy cập dữ liệu và sử dụng các chức năng mà mình cần trong quá trình làm việc của mình. Các ủy quyền phù hợp cũng phải được chỉ định để truy cập vào các tệp là thành phần của hệ điều hành hoặc của các ứng dụng hoặc được tạo ra bởi cùng một hệ điều hành (ví dụ: tệp cấu hình và tệp nhật ký).

Bên cạnh việc truy cập dữ liệu, việc thực thi các ứng dụng và thành phần cũng phải được thực hiện với các quyền ở mức thấp nhất có thể. Các ứng dụng không nên được thực thi với quyền quản trị viên hoặc hệ thống.

Nhận dạng việc xóa tài khoản người dùng

Yêu cầu:

Người dùng sẽ được Bộ định tuyến xác định rõ ràng. Bộ định tuyến sẽ hỗ trợ việc chỉ định các tài khoản cá nhân cho mỗi người dùng, trong đó người dùng có thể là một người hoặc đối với Tài khoản máy, một ứng dụng hoặc một hệ thống. Theo mặc định, bộ định tuyến sẽ không cho phép sử dụng tài khoản nhóm hoặc thông tin đăng nhập nhóm hoặc chia sẻ cùng một tài khoản giữa nhiều người dùng.

Quản lý thuộc tính xác thực

Chính sách xác thực

Yêu cầu:

Việc sử dụng chức năng hệ thống mà không xác thực thành công trên cơ sở nhận dạng người dùng và ít nhất một thuộc tính xác thực (ví dụ: mật khẩu, chứng chỉ) sẽ bị ngăn chặn. Các chức năng hệ thống bao gồm, ví dụ như các dịch vụ mạng (như SSH, SFTP, dịch vụ Web), quyền truy cập cục bộ thông qua bảng điều khiển quản lý, cách sử dụng cục bộ hệ điều hành và ứng dụng.

Yêu cầu này cũng sẽ được áp dụng cho các tài khoản chỉ được sử dụng để liên lạc giữa các hệ thống. Một ngoại lệ đối với yêu cầu xác thực và ủy quyền là các chức năng dành cho mục đích sử dụng công cộng, chẳng hạn như các chức năng dành cho máy chủ Web trên Internet, qua đó thông tin được cung cấp cho công chúng.

Hỗ trợ xác thực

Yêu cầu:

Cơ chế xác thực bên ngoài nếu được sản phẩm Mạng hỗ trợ (hỗ trợ khả năng xác thực, ủy quyền và máy chủ kế toán) phải thông qua kênh liên lạc an toàn (được mã hóa).

Bảo vệ khỏi sự tấn công bên ngoài

Yêu cầu:

Nếu mật khẩu được sử dụng làm thuộc tính xác thực thì phải triển khai biện pháp bảo vệ chống lại các cuộc tấn công từ điển và vũ lực gây cản trở việc đoán mật khẩu. Các cuộc tấn công từ điển và bạo lực nhằm mục đích sử dụng tính năng đoán tự động để xác định mật khẩu cho tài khoản người dùng và máy. Có thể thực hiện nhiều biện pháp khác nhau hoặc kết hợp các biện pháp này để ngăn chặn điều này. Các biện pháp bảo vệ được sử dụng phổ biến nhất là:

(i) Sử dụng độ trễ hẹn giờ (độ trễ này có thể bằng hoặc tăng lên tùy thuộc vào chính sách của nhà điều hành cho mỗi lần thử) cho mỗi lần nhập mật khẩu mới nhập sau khi nhập sai ("tar pit").

(ii) Chặn tài khoản sau một số lần thử sai nhất định.

Tuy nhiên, phải lưu ý rằng giải pháp này cần một quy trình mở khóa và kẻ tấn công có thể buộc điều này vô hiệu hóa các tài khoản và khiến chúng không thể sử dụng được.

(iii) Sử dụng CAPTCHA để ngăn chặn các nỗ lực tự động (thường được sử dụng cho các ứng dụng Web).

(iv) Sử dụng danh sách đen mật khẩu để ngăn chặn các mật khẩu dễ bị tấn công.

Thực thi mật khẩu mạnh

Yêu cầu:

(a) Cài đặt của nhà cung cấp phải sao cho sản phẩm mạng chỉ chấp nhận mật khẩu tuân thủ các tiêu chí phức tạp sau:

(i) Độ dài tối thiểu tuyệt đối là 8 ký tự (độ dài ngắn hơn sẽ bị sản phẩm mạng từ chối). Không thể đặt độ dài tối thiểu tuyệt đối này thành giá trị thấp hơn theo cấu hình.

(ii) Gồm ít nhất ba trong số các loại sau:

- ít nhất 1 ký tự viết hoa (A-Z)

- ít nhất 1 ký tự chữ thường (a-z)

- ít nhất 1 chữ số (0-9)

- ít nhất 1 ký tự đặc biệt (ví dụ: @;!$.)

Độ dài tối thiểu của các ký tự trong mật khẩu và tập hợp các ký tự đặc biệt được phép sẽ do người vận hành cấu hình. Độ dài tối thiểu mặc định là giá trị được nhà cung cấp định cấu hình trước khi áp dụng bất kỳ cấu hình dành riêng cho nhà điều hành nào. Các ký tự đặc biệt có thể được phân loại theo bộ theo danh mục Unicode của chúng.

Nếu hệ thống trung tâm được sử dụng để thực hiện chính sách mật khẩu xác thực người dùng trên hệ thống trung tâm thì phải cung cấp thêm sự đảm bảo rằng hệ thống trung tâm thực thi các quy tắc về độ phức tạp của mật khẩu giống như được đặt ra cho hệ thống cục bộ trong điều khoản này. Nếu hệ thống trung tâm không được sử dụng để xác thực người dùng thì việc đảm bảo các quy tắc về độ phức tạp của mật khẩu sẽ được thực hiện trên Sản phẩm Mạng.

Khi người dùng thay đổi mật khẩu hoặc nhập mật khẩu mới, hệ thống sẽ kiểm tra và đảm bảo rằng mật khẩu đó đáp ứng các yêu cầu về mật khẩu. Các yêu cầu trên sẽ được áp dụng cho tất cả mật khẩu được sử dụng (ví dụ: cấp ứng dụng, cấp hệ điều hành, v.v.).

Hết thời gian phiên không hoạt động

Yêu cầu:

(a) Phiên tương tác của người dùng OAM sẽ tự động bị chấm dứt sau một khoảng thời gian không hoạt động được chỉ định. Có thể định cấu hình khoảng thời gian chờ không hoạt động.

LƯU Ý: Loại hoạt động cần thiết để đặt lại bộ hẹn giờ hết thời gian chờ tùy thuộc vào loại phiên của người dùng.

Thay đổi mật khẩu

Yêu cầu:

Nếu mật khẩu được sử dụng làm thuộc tính xác thực thì hệ thống sẽ cung cấp chức năng cho phép người dùng thay đổi mật khẩu của mình bất kỳ lúc nào. Khi sử dụng hệ thống tập trung bên ngoài để xác thực người dùng, có thể chuyển hướng hoặc triển khai chức năng này trên hệ thống này.

Việc thay đổi mật khẩu sẽ được thực thi sau lần đăng nhập đầu tiên.

Hệ thống sẽ thực thi việc thay đổi mật khẩu dựa trên chính sách quản lý mật khẩu. Đặc biệt, hệ thống sẽ thực thi hết hạn mật khẩu.

Mật khẩu đã sử dụng trước đây không được phép đạt tới một con số nhất định (Lịch sử mật khẩu).

Số lượng mật khẩu không được phép sử dụng trước đây sẽ là:

• Có thể cấu hình;

• Lớn hơn 0;

• Và giá trị mặc định của nó sẽ là 3. Điều này có nghĩa là sản phẩm Mạng sẽ lưu trữ ít nhất ba mật khẩu đã đặt trước đó. Số lượng mật khẩu tối đa mà sản phẩm mạng có thể lưu trữ cho mỗi người dùng tùy thuộc vào nhà sản xuất.

Khi mật khẩu sắp hết hạn, người dùng sẽ nhận được thông báo hết hạn mật khẩu. Các yêu cầu trên sẽ được áp dụng cho tất cả mật khẩu được sử dụng (ví dụ: cấp ứng dụng, cấp hệ điều hành, v.v.). Một ngoại lệ cho yêu cầu này là tài khoản máy.

Yêu cầu này phải được đáp ứng bởi chính sản phẩm Mạng hoặc kết hợp với hệ thống xác thực bên ngoài.

Phản hồi xác thực được bảo vệ

Yêu cầu:

(a) Các thuộc tính Xác thực sẽ không được hiển thị theo cách mà người quan sát cục bộ bình thường có thể nhìn thấy và sử dụng sai. Thông thường, các nhân vật riêng lẻ của mật khẩu được thay thế bằng một ký tự như "*". Trong một số trường hợp nhất định, có thể cho phép hiển thị ngắn gọn một ký tự riêng lẻ trong quá trình nhập. Ví dụ, chức năng như vậy được sử dụng trên điện thoại thông minh để giúp việc nhập liệu dễ dàng hơn. Tuy nhiên, toàn bộ mật khẩu không bao giờ được xuất ra màn hình dưới dạng văn bản gốc.

Các yêu cầu trên sẽ được áp dụng cho tất cả các thuộc tính xác thực được sử dụng (ví dụ: cấp ứng dụng, cấp hệ điều hành, v.v.).

Loại bỏ các thuộc tính xác thực mặc định hoặc xác thực được xác định trước

Yêu cầu:

Các thuộc tính xác thực mặc định hoặc được xác định trước sẽ bị xóa hoặc vô hiệu hóa.

Thông thường, các thuộc tính xác thực như mật khẩu hoặc khóa mật mã sẽ được cấu hình sẵn từ nhà sản xuất, nhà cung cấp hoặc nhà phát triển hệ thống. Các thuộc tính xác thực như vậy sẽ được thay đổi bằng cách tự động buộc người dùng thay đổi khi đăng nhập lần đầu vào hệ thống hoặc nhà cung cấp cung cấp hướng dẫn cách thay đổi thủ công.

Bảo mật phần mềm

Cập nhật

Yêu cầu:

Các bản cập nhật phần mềm hệ thống của sản phẩm mạng phải an toàn và phải dựa trên các chứng chỉ đã ký. Sản phẩm mạng chỉ cho phép cập nhật nếu chứng chỉ ký mã hợp lệ và thời gian chưa hết hạn, tính toàn vẹn của bản cập nhật phần mềm phải được xác minh bằng cơ chế băm (như SHA2).

Nâng cấp an toàn

Yêu cầu:

(i) Tính toàn vẹn của gói phần mềm phải được xác nhận trong giai đoạn cài đặt/nâng cấp.

(ii) Sản phẩm mạng phải hỗ trợ xác thực tính toàn vẹn của gói phần mềm thông qua các phương tiện mật mã, ví dụ: chữ ký số. Để đạt được mục đích này, sản phẩm mạng có danh sách khóa công khai hoặc chứng chỉ của các nguồn phần mềm được ủy quyền và sử dụng khóa để xác minh rằng bản cập nhật phần mềm chỉ bắt nguồn từ những nguồn này.

(iii) Phần mềm giả mạo sẽ không được thực thi hoặc cài đặt nếu quá trình kiểm tra tính toàn vẹn không thành công.

(iv) Cần có cơ chế bảo mật để đảm bảo rằng chỉ những cá nhân được ủy quyền mới có thể bắt đầu và triển khai bản cập nhật phần mềm cũng như sửa đổi danh sách được đề cập trong mục 2

Đảm bảo an toàn mã nguồn

Yêu cầu:

Nhà cung cấp phải đảm bảo những điều sau khi phát triển Hệ điều hành/Phần mềm ứng dụng của sản phẩm Mạng

(i) Các biện pháp thực hành tốt nhất theo tiêu chuẩn ngành về mã hóa an toàn trong toàn bộ vòng đời phát triển phần mềm của Phần mềm sản phẩm Mạng, bao gồm mã do nhà cung cấp phát triển, phần mềm của bên thứ ba và các thư viện mã nguồn mở được sử dụng/nhúng trong sản phẩm Mạng

(ii) Phần mềm sản phẩm Mạng không có các lỗ hổng bảo mật đã biết, các điểm yếu bảo mật được liệt kê trong cơ sở dữ liệu CWE và tất cả các lỗ hổng bảo mật có thể khai thác được liệt kê trong SANS Top 25 và OWASP Top 10 mới nhất

(iii) Tệp nhị phân cho ứng dụng sản phẩm Mạng được tạo từ mã nguồn không có tất cả các lỗ hổng bảo mật mã hóa đã nêu

Kiểm tra phần mềm độc hại

Yêu cầu:

Nhà cung cấp phải gửi Tài liệu Kiểm tra Phần mềm (STD) của sản phẩm mạng để chứng minh rằng sản phẩm mạng không có phần mềm độc hại/phần mềm gián điệp đã biết cho phòng thí nghiệm để giám sát

Phần mềm không được sử dụng

Yêu cầu:

Các thành phần phần mềm không sử dụng hoặc các bộ phận của phần mềm không cần thiết cho hoạt động hoặc chức năng của sản phẩm Mạng sẽ không được cài đặt hoặc sẽ bị xóa sau khi cài đặt. Điều này cũng bao gồm các phần của phần mềm, sẽ được cài đặt làm ví dụ nhưng thường không được sử dụng (ví dụ: các trang web mặc định, cơ sở dữ liệu mẫu, dữ liệu thử nghiệm).

Loại bỏ dịch vụ không cần thiết

Yêu cầu:

Sản phẩm Mạng sẽ chỉ chạy các trình xử lý giao thức và các dịch vụ cần thiết cho hoạt động của nó và không có bất kỳ lỗ hổng bảo mật nào đã biết. Cụ thể, theo mặc định, các dịch vụ sau đây ban đầu sẽ được nhà cung cấp cấu hình để vô hiệu hóa trên sản phẩm Mạng.

- FTP

- TFTP

- Telnet

- Đăng nhập, RCP, RSH

- HTTP

- SNMPv1 và v2

- SSHv1

- Máy chủ nhỏ TCP/UDP (Echo, Chargeen, Discard và Daytime

- Máy chủ BOOTP

- Giao thức khám phá (CDP, LLDP)

- Dịch vụ nhận dạng IP (Identd)

Nguồn hệ thống

Yêu cầu

Sản phẩm mạng chỉ có thể khởi động từ các thiết bị bộ nhớ dành cho mục đích này (ví dụ: không phải từ bộ nhớ ngoài như khóa USB)

Đồng bộ hóa thời gian

Yêu cầu:

Sản phẩm Mạng phải cung cấp thông tin ngày giờ đáng tin cậy do chính Sản phẩm Mạng cung cấp hoặc thông qua máy chủ NTP. Sản phẩm mạng sẽ tạo nhật ký kiểm tra cho tất cả các thay đổi đối với cài đặt thời gian. Sản phẩm mạng phải hỗ trợ định cấu hình xác thực giữa chính nó và máy chủ NTP bên ngoài

Tự kiểm tra

Yêu cầu

Sản phẩm mạng phải thực hiện tự kiểm tra để xác định các lỗi trong Cơ chế bảo mật của nó trong quá trình i)bật nguồn ii) khi Quản trị viên hướng dẫn. (ví dụ: tính toàn vẹn của phần sụn và phần mềm cũng như hoạt động chính xác của các chức năng mã hóa, v.v.)

Khả năng tiếp cận dịch vụ bị hạn chế

Yêu cầu:

Sản phẩm mạng phải hạn chế khả năng tiếp cận của các dịch vụ để chỉ có thể tiếp cận chúng trên các giao diện yêu cầu sử dụng chúng. Trên các giao diện là các dịch vụ đang hoạt động, khả năng tiếp cận phải được giới hạn ở các giao tiếp ngang hàng hợp pháp. Hạn chế này sẽ được hiện thực hóa trên chính sản phẩm mạng.

VÍ DỤ: Các dịch vụ quản trị (ví dụ: SSH, HTTPS, RDP) sẽ bị hạn chế ở các giao diện trong mạng quản lý để hỗ trợ tách biệt lưu lượng quản lý khỏi lưu lượng người dùng.

Truy cập không dây

Yêu cầu

Cam kết sẽ được đưa ra như sau: "Sản phẩm Mạng không chứa bất kỳ thành phần không dây, quang học, từ tính hoặc bất kỳ thành phần nào khác có thể được sử dụng làm kênh bí mật"

Lưu ý: Ngoài các thử nghiệm liên quan đến công nghệ không dây, sản phẩm mạng hỗ trợ các công nghệ không dây tiêu chuẩn cũng cần phải được kiểm tra theo yêu cầu này.

(4)

CHỨNG NHẬN AN NINH VIỄN THÔNG

Doc. No.: NCCS/SC/01/30032020

GIỚI THIỆU

Quy tắc Điện báo Ấn Độ, 1951, PHẦN XI, Kiểm tra & Chứng nhận Điện báo, (Quy tắc 528 đến 537) quy định rằng mọi thiết bị Viễn thông đều phải trải qua quá trình kiểm tra và chứng nhận bắt buộc trước đó.

Trong bối cảnh đó, Cục Viễn thông đã ban hành tài liệu vide "Chương trình chứng nhận an ninh truyền thông" số NCCS/ComSec/01/30032020 về Chứng nhận bảo mật cho thiết bị viễn thông.

Tài liệu cấp dưới này đưa ra quy trình chi tiết để kiểm tra bảo mật và chứng nhận thiết bị Viễn thông.

Bất kỳ Nhà sản xuất thiết bị gốc (OEM)/nhà nhập khẩu/đại lý/Nhà cung cấp dịch vụ nào muốn bán, nhập khẩu hoặc sử dụng bất kỳ thiết bị Viễn thông nào ở Ấn Độ đều phải có Chứng chỉ bảo mật từ Trung tâm An ninh Truyền thông Quốc gia (NCCS).

Quá trình chứng nhận nỗ lực đảm bảo rằng thiết bị Viễn thông tuân thủ các tiêu chuẩn và yêu cầu bảo mật Viễn thông thiết yếu của từng quốc gia, cụ thể là Yêu cầu Đảm bảo An ninh Viễn thông Ấn Độ (ITSAR).

Định nghĩa

Tất cả các định nghĩa trong tài liệu " Chương trình chứng nhận an ninh truyền thông" sẽ được áp dụng

"Đại diện được ủy quyền của Ấn Độ có nghĩa là một công ty hoặc công ty được thành lập ở Ấn Độ, trong trường hợp thiết bị nhập khẩu, đã được OEM nước ngoài ủy quyền hợp lệ để thực hiện tất cả các nghĩa vụ được yêu cầu theo MTCTE đối với thiết bị nhập khẩu

'BoM' có nghĩa là Bill of Material, và là một tập tin chứa thông tin chi tiết về tất cả các mô-đun/thành phần chính của mô hình đang được cung cấp để thử nghiệm. Trường hợp hồ sơ đề nghị chứng nhận nhiều mẫu xe thì HĐQT phải đưa vào nội dung chi tiết của tất cả các mẫu xe.

Phạm vi chứng nhận

Bảo mật sẽ bao gồm tất cả các loại thiết bị Viễn thông được bán ở Ấn Độ hoặc được kết nối với mạng Viễn thông Ấn Độ có ITSTAR sẵn có và có hiệu lực.

Ngày có hiệu lực của việc chứng nhận trở thành bắt buộc đối với các thiết bị Viễn thông khác nhau sẽ được Chính phủ thông báo riêng.

Việc sử dụng thiết bị được chứng nhận, trừ khi được miễn trừ cụ thể, sẽ phải tuân theo các hướng dẫn và quy tắc hiện hành.

Nếu thiết bị được nhập khẩu để nghiên cứu và phát triển hoặc nhằm mục đích trình diễn ở Ấn Độ hoặc làm mẫu để thử nghiệm bắt buộc thì chứng nhận an ninh trước có thể được miễn đối với số lượng thiết bị hạn chế.

Bất kỳ thiết bị không được chứng nhận nào, không bị luật pháp nào cấm ở Ấn Độ, được đích thân đi cùng trong chuyến du lịch nước ngoài tới Ấn Độ để sử dụng cho mục đích cá nhân, có thể được miễn kiểm tra và chứng nhận bắt buộc khi tự công bố.

TỔNG QUÁT

Bất kỳ OEM/nhà nhập khẩu/đại lý/người sử dụng thiết bị Viễn thông nào trước tiên phải đảm bảo rằng mẫu thiết bị mình định bán hoặc sử dụng được chứng nhận theo Chương trình này.

Giấy chứng nhận chỉ cần được cấp một lần cho một 'kiểu' thiết bị và được áp dụng cho bất kỳ số lượng nào của kiểu thiết bị được chứng nhận. Một mẫu thiết bị khác cần có chứng nhận riêng.

Model có cấu hình đầy đủ về phần cứng, giao diện và phần mềm được gọi là Main model. Các mô hình liên kết nhằm mục đích chứng nhận Bảo mật là những mô hình có phần mềm giống hệt nhau nhưng có phần cứng là tập hợp con của mô hình chính. Các mẫu thiết bị viễn thông đi kèm phải được chứng nhận mà không cần thử nghiệm.

Chỉ những thiết bị độc lập, hoàn chỉnh mới được thử nghiệm và chứng nhận theo chương trình này. Các mô-đun/thành phần thiết bị không nằm trong phạm vi chương trình. Hơn nữa, sự kết hợp của các thiết bị độc lập được tạo thành hệ thống không được chứng nhận theo chương trình này; thay vào đó, mỗi thiết bị độc lập sẽ cần có chứng nhận riêng.

Giấy chứng nhận có giá trị trong 5 năm kể từ ngày cấp.

NCCS có thể đình chỉ/hủy bỏ chứng chỉ nếu NCCS biết được bất kỳ vi phạm nào đối với các hướng dẫn và quy tắc hiện hành.

NCCS có thể ban hành các hướng dẫn như vậy cho các OEM/nhà nhập khẩu/đại lý/người dùng phù hợp với Đạo luật, Quy tắc hoặc thủ tục này, nếu cần, để quy trình chứng nhận hoạt động trơn tru.

Các thủ tục chứng nhận an ninh được trình bày chi tiết trong tài liệu này có thể được sửa đổi theo thời gian.

QUY TRÌNH CHỨNG NHẬN

Quy trình Chứng nhận Bảo mật nói chung bao gồm hai phần; thứ nhất, thử nghiệm dựa trên ITSAR hiện hành và thứ hai là đánh giá kết quả thử nghiệm để đảm bảo sự phù hợp với các yêu cầu này. Nếu thiết bị được phát hiện tuân thủ tất cả ITSAR hiện hành, thiết bị đó sẽ được chứng nhận về hiệu quả đó.

Bất kỳ người nộp đơn nào muốn được chứng nhận theo chương trình này đều có thể đăng ký trực tuyến trên cổng thông tin MTCTE (https://www.mtcte.tec.gov.in). Người nộp đơn có thể cung cấp các tài liệu liên quan như (i) Đăng ký công ty (ii) Thư do công ty ủy quyền cho anh ta cấp đối với các trách nhiệm liên quan. Ngoài ra, trong trường hợp OEM nước ngoài, người nộp đơn từ công ty Ấn Độ phải cung cấp tài liệu hỗ trợ (iii) Biên bản ghi nhớ giữa OEM nước ngoài và đại diện Ấn Độ (AIR) để bán và hỗ trợ sản phẩm ở Ấn Độ và (iv) ủy quyền cho AIR cho liên quan đến MTCTEresponsibilities.

Các tài liệu sẽ được xem xét kỹ lưỡng và bất kỳ thiếu sót nào trong tài liệu sẽ được thông báo cho người nộp đơn. Sau khi khắc phục những thiếu sót, đăng ký của người nộp đơn sẽ được phê duyệt, sau đó người nộp đơn có thể nộp đơn đăng ký kiểm nghiệm/chứng nhận.

Người nộp đơn phải chọn sản phẩm cần được chứng nhận, chi tiết về biến thể, giao diện có sẵn và thông tin về các kiểu máy liên quan, nếu có, đồng thời tải tệp Hóa đơn Vật liệu (BoM) lên cổng thông tin. BoM nhằm mục đích chứng nhận bảo mật sẽ bao gồm phiên bản Phần mềm của Hệ điều hành, Cơ sở dữ liệu, mô-đun Mật mã và bất kỳ phần mềm độc quyền/bên thứ ba nào khác được sử dụng trong thiết bị ngoài các chi tiết phần cứng khác. Sau khi nộp đơn, ITSAR hiện hành và phí phải trả sẽ được thông báo/hiển thị cho

Sau khi thanh toán phí áp dụng, người nộp đơn phải kiểm tra thiết bị của mình dựa trên ITSAR hiện hành từ bất kỳ TSTL nào được chỉ định. TSTL được yêu cầu phải hoàn thành bài kiểm tra trong khoảng thời gian 16 tuần, bao gồm bất kỳ khoảng thời gian nào mà người nộp đơn yêu cầu để giải quyết mọi hành vi không tuân thủ phát sinh trong quá trình kiểm tra.

NCCS có thể chỉ định người xác thực để giám sát kỹ thuật đối với thử nghiệm được thực hiện trong TSTL.

Sau khi hoàn thành quá trình kiểm tra, TSTL sẽ tải lên các báo cáo Kiểm tra cùng với ký hiệu của thiết bị được kiểm tra. Bản cứng của thử nghiệm báo cáo cũng sẽ được chuyển đổi cho các đơn vị NCCS. Báo cáo thử nghiệm phải được NCCS đánh giá về khả năng thực hiện ITSAR độ thủ công.

Nếu thiết bị được phát hiện tuân thủ (các) ITSAR hiện hành thì Giấy chứng nhận sẽ được cấp cho người nộp đơn đối với mẫu thiết bị cụ thể.

Chứng chỉ thường sẽ được cấp trong vòng 4-8 tuần kể từ ngày nộp kết quả kiểm tra đầy đủ, tùy thuộc vào độ phức tạp của thiết bị.

Nếu ITSAR được sửa đổi và một phiên bản mới của ITSAR được phát hành, phiên bản đó sẽ được áp dụng kể từ ngày dự kiến được nêu trong phiên bản mới của ITSAR. Cho đến thời điểm đó, ITSAR hiện tại sẽ được áp dụng.

Bạn có thể liên hệ với Trung tâm Kỹ thuật Viễn thông (TEC) hoặc bất kỳ tổ chức nào khác được chỉ định để làm rõ các vấn đề liên quan đến quy trình đăng ký.

Phí phải trả

Phí được tính theo Chương trình sẽ bao gồm Phí đánh giá báo cáo kiểm tra bảo mật được đưa ra dưới đây. Khoản phí này phải được thanh toán cao hơn mức phí do TEC quy định theo Biểu phí được nêu trong phiên bản mới nhất của tài liệu TEC MTCTE "Quy trình thử nghiệm và chứng nhận":

Nhóm thiết bị Bảo mật Báo cáo thử nghiệm Phí đánh giá	Phí đánh giá báo cáo kiểm tra bảo mật
A và B	2,00,000
C	2,50,000
D	3,50,000

Phí đánh giá báo cáo kiểm tra bảo mật nêu trên cũng sẽ được áp dụng cho việc sửa đổi Chứng chỉ liên quan đến kiểm tra bảo mật.

Phí gia hạn sẽ được áp dụng nếu đơn xin gia hạn chứng chỉ được thực hiện và không liên quan đến việc kiểm tra hoặc đánh giá báo cáo. Số tiền phí này giống như phí Hành chính đối với nhóm sản phẩm tương ứng.

Trong trường hợp vá lỗi/sửa lỗi/cập nhật Phần mềm, chủ chứng chỉ chịu trách nhiệm xác định sự tuân thủ của thiết bị được chứng nhận, bao gồm cả thiết bị đã triển khai, với ITSAR và nộp đơn xin sửa đổi chứng chỉ. Bất cứ khi nào một bản vá/sửa lỗi/cập nhật được OEM phát hành, nó có thể được phép triển khai cùng với chứng chỉ tạm thời. OEM sẽ gửi chữ ký đã thay đổi cùng với tất cả các báo cáo thử nghiệm nội bộ thể hiện sự tuân thủ tất cả các yêu cầu bảo mật của ITSAR hiện hành cùng với cam kết được đưa ra trong Phụ lục. Chữ ký đã sửa đổi của mẫu xe nói trên sẽ được đưa vào chứng chỉ tạm thời có thời hạn hiệu lực tối đa một năm kể từ ngày phát hành hoặc trong khoảng thời gian còn lại của chứng chỉ ban đầu, tùy theo điều kiện nào đến trước. Giấy chứng nhận tạm thời sẽ được cấp trong vòng 7 ngày làm việc kể từ ngày nộp đơn thông thường. Mọi yêu cầu sửa đổi giấy chứng nhận tạm thời tiếp theo sẽ được cho phép với giá trị hiệu lực trong khoảng thời gian còn lại của giấy chứng nhận đó.

Trong trường hợp bản vá/sửa lỗi/cập nhật Phần mềm ảnh hưởng đến bất kỳ Chức năng bảo mật nào, việc chứng nhận lại sẽ là cần thiết theo khoản 7.3.

Những sửa đổi có thể được phân biệt là thay đổi gia tăng sẽ được phép trải qua thử nghiệm gia tăng.

Bất kỳ sửa đổi nào đối với sản phẩm được chứng nhận mà không có chứng chỉ hợp lệ sẽ được coi là sử dụng thiết bị không được chứng nhận và sẽ bị xử lý tương ứng.

Sự đổi mới

Để gia hạn, chủ Giấy chứng nhận phải đăng ký trực tuyến và thanh toán phí gia hạn ít nhất một tháng trước khi hết thời hạn hiệu lực của giấy chứng nhận hiện tại.

Giấy chứng nhận chỉ được gia hạn nếu không có thay đổi nào trong ITSAR áp dụng cho thiết bị và không có thay đổi nào về kiểu thiết bị.

Sau khi đánh giá đơn xin gia hạn, một giấy chứng nhận mới có giá trị trong 5 năm nữa sẽ được cấp, trong đó ghi rõ số giấy chứng nhận trước đó.

Sửa đổi của ITSAR

Sự phát triển công nghệ, các yêu cầu cụ thể của quốc gia, những thay đổi trong tiêu chuẩn quốc tế hoặc các yêu cầu pháp lý khác có thể đòi hỏi phải sửa đổi ITSAR.

Một phiên bản mới của ITSAR thường sẽ được phát hành cùng với ngày có hiệu lực dự kiến được nêu rõ trên đó.

Việc sửa đổi ITSAR nói chung sẽ không ảnh hưởng đến hiệu lực của chứng chỉ Thiết bị viễn thông đã được chứng nhận cho đến ngày có thông báo về hiệu lực của phiên bản ITSAR mới, sau đó thiết bị sẽ được chứng nhận theo phiên bản mới của ITSAR. Phiên bản mới của ITSAR sẽ cho biết, đối với thiết bị được chứng nhận theo phiên bản ITSAR trước đó, liệu

thiết bị yêu cầu phải trải qua thử nghiệm đầy đủ hoặc tăng dần để được chứng nhận theo phiên bản mới của ITSAR. Thiết bị nhận được đơn đăng ký sau ngày thông báo về hiệu lực của ITSAR sửa đổi phải được chứng nhận theo ITSAR sửa đổi. Tuy nhiên, Chính phủ Ấn Độ có thể chỉ đạo người sở hữu chứng chỉ kiểm tra lại các mẫu xe cụ thể.

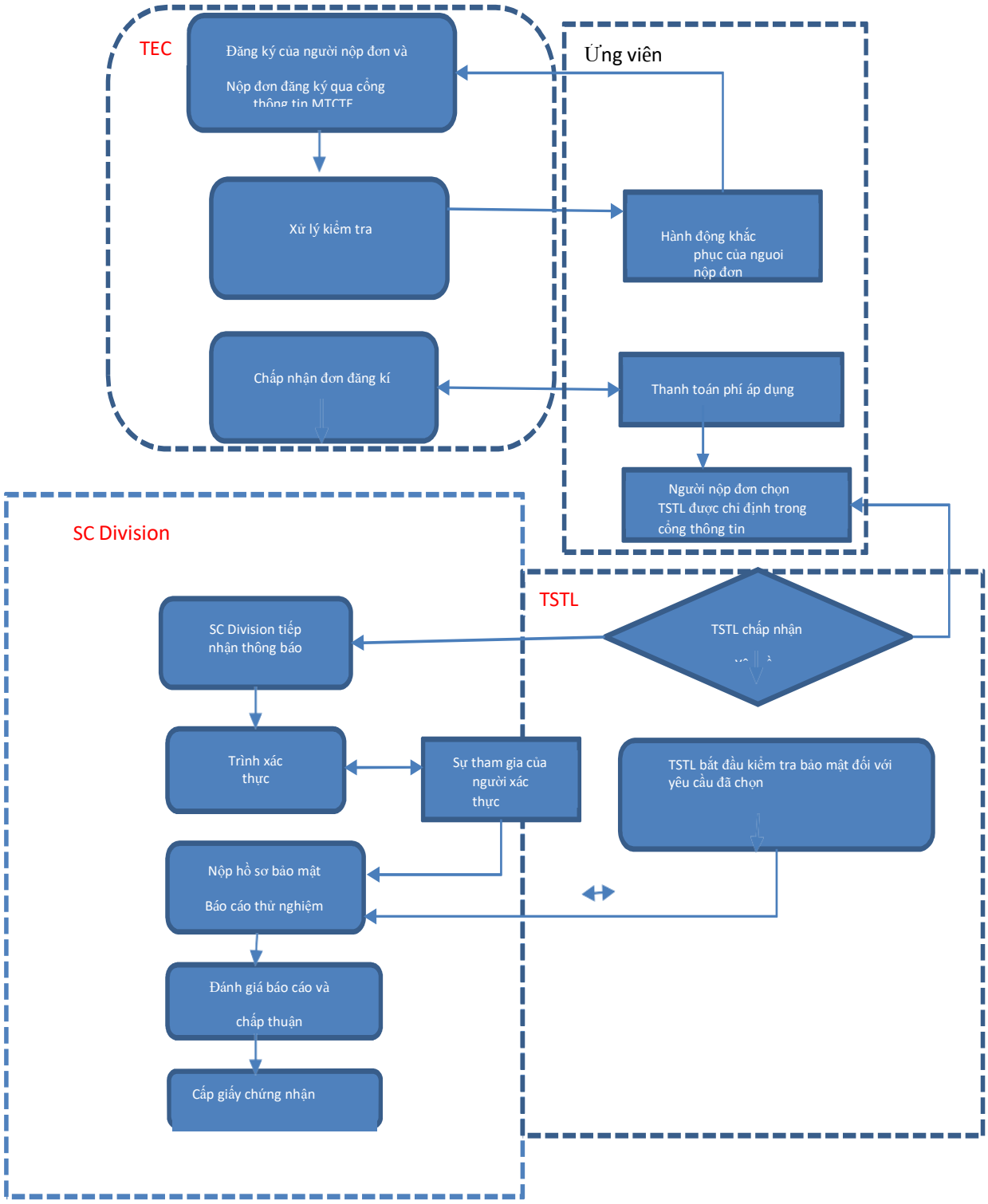
Giám sát

Cơ quan có thẩm quyền (AA) có quyền kiểm tra và/hoặc kiểm tra bất kỳ điện báo nào yêu cầu chứng nhận bắt buộc vào bất kỳ lúc nào và tại bất kỳ cơ sở nào, kể cả địa điểm sử dụng hoặc tại nơi sản xuất để đảm bảo rằng điện báo được sử dụng/bán có các chứng nhận cần thiết và phù hợp với ITSAR của các chứng nhận hiện có. Việc kiểm tra và/hoặc

thử nghiệm như vậy có thể được thực hiện định kỳ hoặc theo quyết định của Cơ quan Điện báo hoặc do bất kỳ khiếu nại nào.

NCCS có thể yêu cầu thử nghiệm lại/đánh giá lại thiết bị viễn thông đã được chứng nhận và tính phí liên quan nếu cần thiết để kiểm tra sự tuân thủ của thiết bị với ITSAR. Những trường hợp này có thể được kiểm tra tại Cơ sở Tiêu chuẩn Đảm bảo An ninh của NCCS hoặc TSTL được chỉ định theo quyết định của Người kiểm soát Chương trình tùy theo từng trường hợp.

Biểu đồ quy trình chứng nhận bảo mật



(5)

THÔNG BÁO

Thông báo về wifi CPE và IP Router (IP tĩnh) bao gồm kiểm tra bảo mật theo MTCTE-redg

Thông báo được đưa ra, bắt đầu chấp nhận các ứng dụng bao gồm kiểm tra bảo mật trên Cổng kiểm tra và chứng nhận bắt buộc thiết bị viễn thông (MTCTE) cho CPE Wifi và Bộ định tuyến IP là ngày 07/01/2023. Do đó, các tham số bảo mật theo Yêu cầu đảm bảo an ninh viễn thông của Ấn Độ (ITSARs) cũng sẽ được áp dụng cho các ứng dụng được gửi trên cổng MTCTE vào hoặc sau ngày 07/01/2023 cùng với các tham số ER cho hai sản phẩm này.

Ngoài ra, các OEM đã được cấp chứng chỉ MTCTE (dựa trên ER) hoặc đang xử lý đơn đăng ký cho các sản phẩm nói trên trước ngày 07/01/2023 cũng phải đăng ký bắt buộc để chuyển đổi chứng chỉ MTCTE của họ sang chứng chỉ tích hợp có kiểm tra bảo mật. Một điều khoản tương tự sẽ được cung cấp thông qua tùy chọn sửa đổi chứng chỉ sau khi cổng MTCTE được đưa vào hoạt động để chấp nhận các ứng dụng bao gồm kiểm tra bảo mật.

Các sản phẩm của ITSAR nói trên và danh sách Phòng thí nghiệm thử nghiệm bảo mật viễn thông (ISTL) được chỉ định để thử nghiệm các sản phẩm nêu trên dựa trên ITSAR hiện hành có sẵn tại trang web NCCS (http://nccs.gov.in).

Các vấn đề trên đều được sự chấp thuận của cơ quan có thẩm quyền.