jtsec

BEYOND IT SECURITY

ETSI EN 303 645

Categories & Provisions

Table of contents

Category	Provision Name	Status	Description
1 REPORTING IMPLEMENTATION	Provision 4.1	M	
2 NO UNIVERSAL DEFAULT PASSWORDS	Provision 5.1-1	MC (1)	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user
	Provision 5.1-2	MC (2)	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device
	Provision 5.1-3	M (8)	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage
	Provision 5.1-4	M C (8)	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used
	Provision 5.1-5	M C (5)	When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable
3 IMPLEMENT A MEANS TO MANAGE REPORTS FOR VULNERABILITIES	Provision 5.2-1	M	The manufacturer shall make a vulnerability disclosure policy publicly available.
	Provision 5.2-2	R	Disclosed vulnerabilities should be acted on in a timely manner.
	Provision 5.2-3	R	Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.
	Provision 5.3-1	R	All software components in consumer IoT devices should be securely updateable

4 KEEP SOFTWARE UPDATED	Provision 5.3-2	M C (5)	When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.
	Provision 5.3-3	M C (12)	An update shall be simple for the user to apply.
	Provision 5.3-4	R C (12)	Automatic mechanisms should be used for software updates
	Provision 5.3-5	R C (12)	The device should check after initialization, and then periodically, whether security updates are available
	Provision 5.3-6	R C (9, 12)	If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications
	Provision 5.3-7	M C (12)	The device shall use best practice cryptography to facilitate secure update mechanisms
	Provision 5.3-8	M C (12)	Security updates shall be timely
	Provision 5.3-9	R C (12)	The device should verify the authenticity and integrity of software updates.
	Provision 5.3-10	M (11, 12)	Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship
	Provision 5.3-11	R C (12)	The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update
	Provision 5.3-12	R C (12)	The device should notify the user when the application of a software update will disrupt the basic functioning of the device.
	Provision 5.3-13	M	The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period
	Provision 5.3-14	R C (3, 4)	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined

			support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.
	Provision 5.3-15	R C (3, 4)	For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.
	Provision 5.3-16	M	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface
5 SECURELY STORE SENSITIVE SECURITY PARAMETERS	Provision 5.4-1	M C (14)	Sensitive security parameters in persistent storage shall be stored securely by the device.
	Provision 5.4-2	M C (10)	Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software
	Provision 5.4-3	M	Hard-coded critical security parameters in device software source code shall not be used.
	Provision 5.4-4	M C (15)	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices
6 COMMUNICATE SECURELY	Provision 5.5-1	M	The consumer IoT device shall use best practice cryptography to communicate securely.
	Provision 5.5-2	R	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography
	Provision 5.5-3	R	Cryptographic algorithms and primitives should be updateable
	Provision 5.5-4	R C (16)	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface
	Provision 5.5-5	M C (17)	Device functionality that allows security-relevant changes in configuration via a

			network interface shall only be accessible after authentication
	Provision 5.5-6	R C (18)	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.
	Provision 5.5-7	M C (19)	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces
	Provision 5.5-8	M C (20)	The manufacturer shall follow secure management processes for critical security parameters that relate to the device.
7 MINIMIZE EXPOSED ATTACK SURFACES	Provision 5.6-1	M	All unused network and logical interfaces shall be disabled
	Provision 5.6-2	M	In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.
	Provision 5.6-3	R	Device hardware should not unnecessarily expose physical interfaces to attack.
	Provision 5.6-4	M C (13)	Where a debug interface is physically accessible, it shall be disabled in software.
	Provision 5.6-5	R	The manufacturer should only enable software services that are used or required for the intended use or operation of the device.
	Provision 5.6-6	R	Code should be minimized to the functionality necessary for the service/device to operate.
	Provision 5.6-7	R	Software should run with least necessary privileges, taking account of both security and functionality.
	Provision 5.6-8	R	The device should include a hardware-level access control mechanism for memory.
	Provision 5.6-9	R	The manufacturer should follow secure development processes for software deployed on the device.
	Provision 5.7-1	R	The consumer IoT device should verify its software using secure boot mechanisms.

8 ENSURE SOFTWARE INTEGRITY	Provision 5.7-2	R	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function
9 ENSURE THAT PERSONAL DATA IS SECURE	Provision 5.8-1	R C (21)	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.
	Provision 5.8-2	M C (22)	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage
	Provision 5.8-3	M C (23)	All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user
10 MAKE SYSTEMS RESILIENT TO OUTAGES	Provision 5.9-1	R	Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power
	Provision 5.9-2	R	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.
	Provision 5.9-3	R	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.
11 EXAMINE SYSTEM TELEMETRY DATA	Provision 5.10-1	R C (6)	If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.
12 MAKE IT EASY FOR USERS TO DELETE USER DATA	Provision 5.11-1	M C (24)	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.
	Provision 5.11-2	R C (25)	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.

	Provision 5.11-3	R C (26)	Users should be given clear instructions on how to delete their personal data.
	Provision 5.11-4	R C (26)	Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.
13 MAKE INSTALLATION AND MANINTENANCE OF DEVICES EASY	Provision 5.12-1	R	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.
	Provision 5.12-2	R	The manufacturer should provide users with guidance on how to securely set up their device.
	Provision 5.12-3	R	The manufacturer should provide users with guidance on how to check whether their device is securely set up
14 VALIDATE INPUT DATA	Provision 5.13-1	M C (27)	The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices
15 DATA PROTECTION PROVISIONS FOR CONSUMER IOT	Provision 6.1	M C (28)	The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers
	Provision 6.2	M C (7)	Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.
	Provision 6.3	M C (6)	Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.
	Provision 6.4	R C (6)	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.
	Provision 6.5	M C (6)	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is

			collected, how it is being used, by whom, and for what purposes.

Conditions

1) passwords are used;

2) pre-installed unique per device passwords are used;

3) software components are not updateable;

4) the device is constrained;

5) the device is not constrained;

6) telemetry data being collected;

7) personal data is processed on the basis of consumers' consent;

8) the device allowing user authentication;

9) the device supports automatic updates and/or update notifications;

10) a hard-coded unique per device identity is used for security purposes;

11) updates are delivered over a network interface;

12) an update mechanism is implemented;

13) a debug interface is physically accessible;

14) sensitive security parameters are stored persistently;

15) critical security parameters used for integrity and authenticity checks of software updates in device software or for

protection of communication with associated services in device software exist;

16) access to device functionality via a network interface in the initialized state is possible;

17) device functionality that allows security-relevant changes in configuration via a network interface exists;

18) critical security parameters are transmitted;

19) critical security parameters are transmitted via remotely accessible network interfaces;

20) critical security parameters relating to the device exist;

21) personal data is transmitted between a device and a service;

22) sensitive personal data is transmitted between a device and a service;

23) external sensing capabilities exist;

24) user data is stored on the device;

25) personal data is stored on associated services;

26) personal data is stored;

27) data input via user interfaces or transferred via APIs or between networks in services and devices is supported;

28) personal data is processed.