ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

Reference

DTS/CYBER-0039

Keywords

cybersecurity, IoT, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

As more devices in the home connect to the internet, the cyber security of the Internet of Things (IoT) is becoming a growing concern. People entrust their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now becoming connected and need to be designed to withstand cyber threats.

The present document brings together widely considered good practice in security for internet-connected consumer devices in a set of high-level outcome-focused provisions. The objective of the present document is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products.

The provisions are outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products.

The present document is not intended to solve all security challenges associated with consumer IoT. Rather, the focus is on the technical controls and organizational policies that matter most in addressing the most significant and widespread security shortcomings.

As many IoT devices and services process and store personal data, the present document can help in ensuring that these are compliant with the General Data Protection Regulation (GDPR) [i.7]. This present document can also help organizations implement a future EU common cybersecurity certification framework as proposed in the Cybersecurity Act [i.13] and the proposed IoT Cybersecurity Improvement Act in the United States.

The provisions in the present document have been developed following review of published standards, recommendations and guidance on IoT security and privacy [i.1], [i.2], [i.8], [i.9], [i.10], [i.11] and [i.12].

NOTE: Mappings of the landscape of IoT security standards, recommendations and guidance are available. See, for example, Mapping Security & Privacy in the Internet of Things (https://iotsecuritymapping.uk/) and ENISA Baseline Security Recommendations for IoT - Interactive Tool (https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security-recommendations-for-iot-interactive-tool).

1 Scope

The present document specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. A non-exhaustive list of examples include:

- connected children's toys and baby monitors;
- connected safety-relevant products such as smoke detectors and door locks;
- smart cameras, TVs and speakers;
- wearable health trackers;
- connected home automation and alarm systems;
- connected appliances (e.g. washing machines, fridges); and
- smart home assistants.

The present document provides basic guidance for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table A.1 provides a basic mechanism for the reader to give information about the implementation of the provisions.

IoT products primarily intended to be employed in manufacturing, other industrial applications and healthcare are not in scope of the present document.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations".

[i.2] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.3] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".

NOTE Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[i.4] ISO/IEC 29147: "Vulnerability Disclosure".

NOTE Available at https://www.iso.org/standard/45170.html.

[i.5] CSAF: "Common Vulnerability Reporting Framework (CVRF)".

NOTE Available at http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html.

[i.6] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.8] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

[i.9] UK Department for Digital, Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report", March 2018.

NOTE Available at https://www.gov.uk/government/publications/secure-by-design.

[i.10] IoT Security Foundation: "IoT Security Compliance Framework", Release 2 December 2018.

NOTE Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf.

[i.11] GSMA: "GSMA IoT Security Guidelines and Assessment".

NOTE Available at https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

NOTE: It is under development.

[i.13] Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

associated services: digital services that are linked to IoT devices, for example mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs) to services such as messaging

constrained device: device which has physical limitations that limit the ability of the device to process, communicate or store data

EXAMPLE: Limitations to the ability of the device, for example to receive and process software updates, can be due to battery life, processing power, physical access (e.g. if the device is embedded in concrete or otherwise inaccessible), limited functionality, limited memory or limited network bandwidth.

consumer: natural person who is acting for purposes which are outside his trade, business, craft or profession

NOTE: Organizations, including businesses of any size, also use consumer IoT. For example, smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses. The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.

consumer IoT: network-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail and that are typically used in the home or as electronic wearables

device manufacturer: entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other manufacturers

isolable: able to be removed from the network it is connected to, without causing functionality loss, so that any compromise affects only itself; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured

personal data: any information relating to an identified or identifiable natural person

security-sensitive data: data that is relevant to the security of a device or service, for example cryptographic keys, device identifiers and initialization vectors

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
CVD	Coordinated Vulnerability Disclosure
CVRF	Common Vulnerability Reporting Framework
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
EU	European Union
eUICC	embedded Universal Integrated Circuit Card
GDPR	General Data Protection Regulation
GSMA	GSM Association
IoT	Internet of Things
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
TEE	Trusted Execution Environment
TS	Technical Specification
UICC	Universal Integrated Circuit Card

4 Cyber security provisions for consumer IoT

4.1 No universal default passwords

Provision 4.1-1 All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. This has been the source of many security issues in IoT and the practice needs to be discontinued. Following best practice on passwords and other authentication methods is encouraged. Device security can further be strengthened by having unique and immutable identities.

NOTE: For guidance see, for example, the NIST Special Publication on Digital Identity Guidelines, Authentication and Lifecycle Management [i.3].

4.2 Implement a means to manage reports of vulnerabilities

Provision 4.2-1 Companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.

Provision 4.2-2 Disclosed vulnerabilities should be acted on in a timely manner.

A "timely manner" for acting on vulnerabilities varies considerably and is incident specific, however, the de facto standard for the vulnerability process to be completed is within 90 days. A hardware fix can take considerably longer to address than a software fix. Additionally, a fix that has to be deployed to devices can take time to roll out compared with a server software fix.

Provision 4.2-3 Companies should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate as part of the product security lifecycle.

Knowing about a security vulnerability allows companies to respond. Vulnerabilities are expected to be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities can be reported to national authorities. Companies are also encouraged to share information with competent industry bodies.

NOTE 1: Competent industry bodies include the GSMA and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation which references the ISO/IEC 29147 standard on vulnerability disclosure [i.4]. The GSMA's industry level Coordinated Vulnerability Disclosure programme is located at: https://www.gsma.com/cvd.

Coordinated Vulnerability Disclosure (CVD) is standardized by the International Organization for Standardization (ISO), is simple to implement and has been proven to be successful in some large software companies around the world [i.4]. CVD is, however, still not established in the IoT industry and some companies are reticent about dealing with security researchers. CVD provides a way for security researchers to contact companies to inform them of security issues putting the company ahead of the threat of malicious exploitation and giving them an opportunity to resolve vulnerabilities in advance of a public disclosure.

Companies that provide internet-connected devices and services have a duty of care to consumers and third parties who can be harmed by their failure to have a CVD programme in place. Additionally, companies that share this information through industry bodies can assist others who can be suffering from the same problem.

Disclosures can comprise different approaches depending on the circumstances:

- Vulnerabilities related to single products or services: the problem is expected to be reported directly to the affected stakeholder (e.g. device manufacturer, IoT service provider or mobile application developer). The source of these reports can be security researchers or industry peers.
- Systemic vulnerabilities: a stakeholder, such as a device manufacturer, can discover a problem that is potentially systemic. Whilst fixing it in the device manufacturer's own product is crucial, there is significant benefit to industry and consumers from sharing this information. Similarly, security researchers can also seek to report such systemic vulnerabilities. In this case, a relevant competent industry body can coordinate a wider scale response.

NOTE 2: The Common Vulnerability Reporting Framework (CVRF) [i.5] can also be useful to exchange information on security vulnerabilities.

Cyber security threat information sharing can support organizations in developing and producing secure products [i.6].

4.3 Keep software updated

Provision 4.3-1 All software components in consumer IoT devices should be securely updateable.

Provision 4.3-2 The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required.

NOTE 1: The appropriate entity is decided by the relevant jurisdiction.