Act nº 77, of January 5, 2021

Published: Tuesday, 05 January 2021 10:16 | Last updated: Thursday, 21 January 2021 10:48 | Hits: 1333

Note : This text does not replace the one published in the Electronic Service Bulletin on 5/1/2021 .

THE SUPERINTENDENT OF GRANT AND RESOURCES TO THE PROVISION - ANATEL, in the use of the powers conferred on him by Resolution No. 715, of October 23, 2019 , and

CONSIDERING the competence given by Items XIII and XIV of Article 19 of Law No. 9.472 / 97 - General Telecommunications Law;

WHEREAS Article 22 of the Regulations for Conformity Assessment and Homologation of Telecommunications Products, approved by Resolution No. 715, of October 23, 2019;

CONSIDERING the National Cybersecurity Strategy, approved by Decree No. 10,222, of February 5, 2020;

CONSIDERING the General Law on Protection of Personal Data, approved by Law No. 13,709, of August 14, 2018 ;

CONSIDERING the minimum Cybersecurity requirements that must be adopted in the establishment of 5G networks, approved by Normative Instruction No. 4, of March 26, 2020 of the Institutional Security Office of the Presidency of the Republic;

WHEREAS Law No. 12,965, of April 23, 2014 , which establishes principles, guarantees, rights and duties for the use of the Internet in Brazil;

WHEREAS Resolution No. 740, of December 21, 2020 , which approves the Cybersecurity Regulation Applied to the Telecommunications Sector, establishes that the subject of the assessment of the conformity of telecommunications equipment, regarding cybersecurity, must be the object of the procedures conformity assessment and approval of telecommunications products; and

CONSIDERING the case file of process No. 53500.026122 / 2019-70 ,

R E S O L V E S :

Art. 1 To approve the Cybersecurity Requirements for Telecommunications Equipment, as per the Annex to this Act.

Art. 2 This Act enters into force 180 (one hundred and eighty) days after the date of its publication in Anatel's Electronic Services Bulletin.

VINICIUS OLIVEIRA CARAM GUIMARÃES

Superintendent of Granting and Provision of Resources

ANNEX TO ACT No. 77, OF JANUARY 5, 2021

CYBER SECURITY REQUIREMENTS FOR TELECOMMUNICATIONS EQUIPMENT

1. OBJECTIVE AND SCOPE

1.1. Establish a set of cybersecurity requirements for telecommunications equipment to minimize or correct vulnerabilities through *software / firmware updates* or configuration recommendations.

1.1.1. This document covers the products listed in the Telecommunications Products Reference List published by the National Telecommunications Agency that have the function of terminal equipment with an Internet connection or telecommunications network infrastructure equipment.

1.2. In the case of initial certification and homologation of equipment, the homologation application must contain a declaration from the interested party informing which requirements listed in this document the product and its supplier meet.

1.2.1. At any time, through the Market Supervision program, Anatel will be able to assess whether the approved product and its

2.1. Regulations for Conformity Assessment and Homologation of Telecommunications Products, approved by Resolution No. 715, of October 23, 2019 .

2.2. OECD - Enhancing the Digital Security of Products - Draft Scoping Paper (November 2019).

2.3. IEEE Internet Technology Policy Community White Paper - Internet of Things (IoT) Security Best Practices (February 2017).

2.4. IETF - Internet of Things (IoT) Security: State of the Art and Challenges - RFC 8576.

2.5. LAC-BCOP-1 (May / 2019) - Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition.

2.6. Joint document LACNOG-M3AAWG: Current Operating Best Practices on Minimum Security Requirements for the Purchase of Equipment for Subscriber Connection (CPE) LAC-BCOP-1 - May 2019.

2.7. ENISA - Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures (November 2017).

2.8. GSMA IoT Security Guidelines - Complete Document Set.

2.9. ETSI GS NFV-SEC 001 V1.1.1 (2014-10) - Network Functions Virtualization (NFV); NFV Security; Problem Statement .

2.10. GSMA - FS.16 - Network Equipment Security Assurance Scheme - Development and Lifecycle Security Requirements.

2.11. Council to Secure the Digital Economy - The C2 Consensus on IoT Device Security Baseline Capabilities .

2.12. ISO / IEC 27402 - Cybersecurity - IoT security and privacy - Device baseline requirements [DRAFT].

2.13. General Law on Protection of Personal Data, approved by Law No. 13,709, of August 14, 2018.

2.14. FIRST *Vulnerability Coordination SIG / Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure,* accessible *at:* https://www.first.org/global/sigs/vulnerability-coordination .

2.15. Common Vulnerability Scoring System (CVSS), accessible at: https://www.first.org/cvss .

2.16. ETSI EN 303 645 v2.1.1 (2020-06) - *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements* .

2.17. ETSI TS 133 117 V16.5.0 (2020-08) - *Universal Mobile Telecommunications System (UMTS); LTE; Catalog of general security assurance requirements* .

2.18. 3GPP Technical Specification Set: SCAS - *Security Assurance Specifications* , accessible at: https://www.3gpp.org/DynaReport/WiSpec--790015.htm .

2.19. EU 5G Security Toolbox , accessible at: https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security .

3. DEFINITIONS

3.1. Cryptographic algorithms: algorithms based on the science of cryptography, covering encryption / decryption algorithms, cryptographic *hash* algorithms, digital signature algorithms and key exchange algorithms.

3.2. Backdoor : undocumented mechanism contained in the product *software / firmware* that allows unauthorized access to the equipment. The presence of *backdoors* in the final product can be intentional or accidental.

3.3. Customer Premise Equipment (CPE): equipment used to connect subscribers to the telecommunications service provider's network. For the purposes of applying this set of requirements, CPE should be considered as equipment associated with fixed telecommunications services.

3.4. Personal data: the definition contained in the General Law for the Protection of Personal Data is adopted.

3.5. Sensitive personal data: the definition contained in the General Law for the Protection of Personal Data is adopted.

3.6. Firmware : *software* accessible only for reading, programmed in specific purpose hardware and stored functionally independent of the equipment's main storage.

3.7. Supplier: is the applicant for the approval of telecommunications equipment, and may be the national manufacturer of the equipment itself or the national representative of a foreign manufacturer.

3.8. Hashing : mathematical algorithm based on internationally recognized standardization that maps variable length data at the input of a function to a set of fixed length data at the output of the function.

3.9. Appropriate encryption methods: protocols or cryptographic algorithms, based on internationally recognized standardization, in their updated versions. The implementation should allow the selection of updated cipher suites and key sizes, and implement the exclusions specified in the standard for elements considered obsolete.

3.10. Appropriate authentication methods: authentication protocols or algorithms based on internationally recognized standardization, in their updated versions. Different technologies and authentication factors can be used (for example, cryptographic *chip* , *tokens* , biometrics, etc.). The implementation should not use authentication credentials (example: passwords, cryptographic keys) with common values fixed in the source code (*hard-coded*).

3.13. Vulnerability: set of internal factors or potential cause of an unwanted incident, which can result in risk to a system or an organization, which can be prevented by an internal action of information security.

4. GENERAL GUIDELINES

4.1. When requesting the approval of the telecommunications product with Anatel, the applicant must submit a declaration:

a) indicating that the product was developed in compliance with the principle of *security by design;*

b) relating to which requirements of this document the equipment and its supplier meet at that moment; and

c) recognizing that they are aware that cybersecurity requirements are subject to updates, including regulatory and administrative ones, in line with technological development, with the emergence of new threats or vulnerabilities.

4.1.1. The scope of the declaration must consider the different technical characteristics of the equipment (amount of memory, data processing capacity, user interfaces, communication interfaces, characteristics and versions of the software / firmware - not limited to these) and the purposes for which intended, pointing out which requirements are met.

4.1.2. For products falling under the definition of CPE, the declaration must also be guided by the set of requirements contained in reference 2.5 .

4.2. In Market Supervision activities, the Agency will be able to assess whether the product and its supplier maintain compliance with the requirements of this document.

4.3. Identified, in the approved product, any flaw or vulnerability that affects the safety of its users or of the country's telecommunications networks, the Agency will notify the person responsible for the approval to do so, indicating an appropriate term for this purpose, considering the degree of severity of the vulnerability, assessed according to the *Common Vulnerability Scoring System* (CVSS) (reference 2.15).

4.3.1. The deadline for the correction of vulnerabilities may be extended, at the Agency's discretion, based on the weightings presented by the homologation applicant and the complexity of the problem.

4.3.2. Once the period has elapsed without the necessary corrections being verified or without justification accepted by Anatel for not implementing the corrections, the Agency may suspend the approval of the product and indicate the collection or replacement of the same in the market, guaranteed the other regulatory provisions regarding the consumer law.

4.3.3. The suspension of the approval of the equipment will be maintained until the identified vulnerabilities are remedied or until the potential risk to the safety of users or telecommunications services is mitigated, considering the maximum period established in the current regulation.

4.3.4. After the maximum period determined for its suspension, the homologation will be canceled, in case the vulnerability is not solved.

5. CYBER SECURITY REQUIREMENTS FOR TELECOMMUNICATIONS EQUIPMENT

5.1. Requirements for terminal equipment that connect to the Internet and for telecommunications network infrastructure equipment, in their final versions intended for commercialization:

5.1.1. Regarding the *software / firmware update* :

a) Have secure and automated mechanisms for updating *software / firmware* that employ adequate methods of encryption, authentication and integrity verification.

b) Allow users to manually check the availability of *software / firmware updates* and easily implement them.

c) Have mechanisms to inform the user of *software / firmware* changes implemented due to updates, especially those related to security.

d) Preserve the existing settings on the equipment after the update procedure is finished. Changes in the configuration of the equipment can be implemented in the update process only if they result in improvements in the security of the device.

5.1.2. As for remote management:

a) Have a mechanism for remote management and administration that employs appropriate authentication and encryption methods.

b) Implement mechanisms to control access to remote management and administration interfaces, in such a way as to limit access as to the source (for example, specific network segment, selected URL, etc.).

5.1.3. Regarding installation and operation:

a) Implement simplified routines suitable for its installation and configuration, avoiding potential unintended security flaws.

b) By factory default, the device must be configured restrictively instead of permissively. The selection of parameters for the initial factory settings must be based on natively safe options, in line with the principles of security and privacy.

f) provide documentation that describes, at least the name, version and functionality of *software / firmware* and / or operating system, as well as full name and version of each *software* code open to embedded system. Documentation can be in electronic format.

5.1.4. As for access to equipment configuration:

a) Do not use credentials and initial passwords to access your settings that are the same among all devices produced.

b) Do not use initial passwords that are derived from information easily obtained by methods of scanning network data traffic, such as MAC addresses - *Media Access Control* .

c) Force, on the first use, the change of the initial password to access the equipment configuration.

d) Do not allow the use of blank passwords or weak passwords.

e) Have defense mechanisms against exhaustive attempts at unauthorized access (brute force authentication attacks).

f) Ensure that the password recovery mechanisms are robust against attempts to steal credentials.

g) Do not use credentials, passwords and cryptographic keys defined in the *software / firmware* source code itself and which cannot be changed (*hard-coded*).

h) Protect passwords, access keys and credentials stored or transmitted using appropriate encryption or *hashing* methods .

i) Implement routines for closing inactive sessions (*timeout*).

5.1.5. Regarding data communication services:

a) Be free of any test tool or *backdoor* used in the product development processes and unnecessary for its usual operation.

b) Be devoid of any form of undocumented communication, including those for sending equipment usage profile information to manufacturers or to third parties.

c) Be provided with data communication services (service associated with a port / *port*) not usually used disabled, reducing its attack surface.

d) Provide the user with the possibility of disabling communication features and services not essential to the operation or management of the equipment.

5.1.6. Regarding personal data and sensitive personal data, observing the current legislation:

a) Enable the use of appropriate encryption methods for the transmission of sensitive data, including personal information.

b) Enable the use of appropriate encryption methods for the storage of sensitive data, including personal information.

c) Allow users to easily delete their stored personal and sensitive data, enabling the disposal or replacement of equipment without risks of exposure of personal information.

d) Contain in its documentation information to the user about which personal data, sensitive or not, are collected, used and stored.

5.1.7. Regarding the ability to mitigate attacks:

a) Have a mechanism for limiting the rate of outgoing data transmission (*upload*), in addition to what is usually necessary, in order to minimize its use as a vector in attacks on other equipment or systems (denial of service attack).

b) Implement mechanisms to validate the origin address of the data packets, filtering packets with falsified origin addresses (*antispoofin* g filter), especially in the transmission of outgoing data (*upload*).

c) Be designed to mitigate the effects of ongoing denial of service attacks, being resistant to an excessive number of authentication attempts, through, for example: prioritizing their processing capacity to communication sessions already established and authenticated; and limiting the number of concurrent authentication sessions, discarding attempts to establish new sessions when the established limit is exceeded.

6. REQUIREMENTS FOR SUPPLIERS OF TELECOMMUNICATIONS EQUIPMENT

6.1. Requirements for providers of terminal equipment that connect to the Internet and telecommunications network infrastructure equipment:

6.1.1. Have a clear product support policy, especially in relation to making *software / firmware* updates available to fix security vulnerabilities.

6.1.2. Make it clear to the consumer how long and in what situations security updates will be provided for the equipment.

6.1.3. When the equipment has automatic *software / firmware* update processes , ensure that the updates are carried out in phases (in parts of all devices) in order to avoid that unintentional errors of the new *software / firmware* version are distributed simultaneously to all equipment that can be updated.

6.1.6. Have coordinated Vulnerability Disclosure processes implemented based on internationally recognized good practices and recommendations.

6.1.7. Provide a public support channel, through a website in Portuguese, to:

a) Inform about new vulnerabilities identified in their products, mitigation measures and associated security patches;

b) Maintain a history of: identified vulnerabilities, mitigation measures and security corrections;

c) Allow access to security patches and / or new *software / firmware* versions for your products; and

d) Provide manuals and other materials with guidelines related to the configuration, update and safe use of the equipment.

7. FINAL PROVISIONS

7.1. Considering the continuous technological evolution of the telecommunications sector and the incessant appearance of new threats to cybersecurity for telecommunications equipment, this document is subject to updates in order to remain aligned with the state of the art in the sector, the regulations issued by Anatel and other measures adopted by it.

7.2. The supplier's declaration, mentioned in item 4 of this document, must be presented in Portuguese according to the model published on Anatel's website.

7.3. Anatel management responsible for product certification and approval may accept, for the purpose of proving compliance with the requirements listed in this document, statements that the equipment meets international standards or recommendations that have a scope aligned with the Cybersecurity Requirements for Telecommunications Equipment .

7.4. Reading the documents referenced in item 2 (References), including their updates, is strongly recommended.

7.4.1. The *links* to internet pages contained in the references are subject to change, being necessary to search for the documents in the cases in which the *links* are inoperative.