Cyber Security for Consumer Internet of Things (IoT)

Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations UK 2023 No. 1007

Raspberry Pi Ltd

Colophon

© 2024 Raspberry Pi Ltd

This documentation is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND).

build-date: 2024-11-22
build-version: 3dd3273-dirty

Legal disclaimer notice

TECHNICAL AND RELIABILITY DATA FOR RASPBERRY PI PRODUCTS (INCLUDING DATASHEETS) AS MODIFIED FROM TIME TO TIME ("RESOURCES") ARE PROVIDED BY RASPBERRY PI LTD ("RPL") "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN NO EVENT SHALL RPL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE RESOURCES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RPL reserves the right to make any enhancements, improvements, corrections or any other modifications to the RESOURCES or any products described in them at any time and without further notice.

The RESOURCES are intended for skilled users with suitable levels of design knowledge. Users are solely responsible for their selection and use of the RESOURCES and any application of the products described in them. User agrees to indemnify and hold RPL harmless against all liabilities, costs, damages or other losses arising out of their use of the RESOURCES.

RPL grants users permission to use the RESOURCES solely in conjunction with the Raspberry Pi products. All other use of the RESOURCES is prohibited. No licence is granted to any other RPL or other third party intellectual property right.

HIGH RISK ACTIVITIES. Raspberry Pi products are not designed, manufactured or intended for use in hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems or safety-critical applications (including life support systems and other medical devices), in which the failure of the products could lead directly to death, personal injury or severe physical or environmental damage ("High Risk Activities"). RPL specifically disclaims any express or implied warranty of fitness for High Risk Activities and accepts no liability for use or inclusions of Raspberry Pi products in High Risk Activities.

Raspberry Pi products are provided subject to RPL's Standard Terms. RPL's provision of the RESOURCES does not expand or otherwise modify RPL's Standard Terms including but not limited to the disclaimers and warranties expressed in them.

Table of contents

Chapter 1. Connected Device Security and the Internet of Things (IoT)

The topic of IoT security (or the lack thereof) has been a subject of governmental and international debate for the past ten years. Cyberattacks involving internet-enabled 'smart devices' include the invasion of privacy, fraud, and the weaponization of internet traffic. Examples of the latter include botnet attacks, where large numbers of distributed devices are collectively used to disrupt internet traffic through denial-of-service attacks.

1.1. The Product Security and Telecommunications Infrastructure Act 2022 (PSTI)

In response to security concerns, the Product Security and Telecommunications Infrastructure Act 2022 **(PSTI Act 2022)** was passed. Acts of Parliament cover a range of topics and are used to establish the legal rights and obligations of individuals and organisations within the UK. The PTSI became law in December 2022, establishing legal rights for individuals relevant to the cybersecurity of consumer-connectable products.

1.2. Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations

Acts of Parliament often authorise the government to create more specific rules and regulations, known as delegated legislation. This helps to provide more detail to the law, and more flexibility in implementing it. The PSTI is no different, and the Product Security and Telecommunications Infrastructure **(Security Requirements for Relevant Connectable Products)** Regulations became law in 2023. The Regulation provides more detailed information on the security requirements of IoT devices, establishing three aspects of cybersecurity intended to protect consumers:

Passwords

Universal default passwords and easily guessable passwords are prohibited. This means each device must have a unique and secure password, or allow users to create their own strong passwords.

Vulnerability Reporting

Manufacturers must provide a clear way for users to report security vulnerabilities in their products. This allows for quicker identification and patching of security holes.

Security Updates

Manufacturers are required to publish information on the minimum period for which they will provide security updates for their products. This ensures that consumers know how long their devices will be actively supported with security patches.

1.3. Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645 V2.1.1)

Even with the added detail provided by the Regulation, designers of IoT devices were not given a specific set of rules

that would allow them to presume conformity to the regulation. In answer to this, the European Telecommunications Standards Institute (ETSI) established a Technical Committee on Cybersecurity (TC CYBER) to engage with industry and consumer stakeholders, and the '**ETSI EN 303 645 V2.1.1** Standard Cyber Security for Consumer Internet of Things: Baseline Requirements' was published in collaboration. This standard is publicly available and free to access. A summary of the standard reads:

Purpose

The standard aims to improve the cybersecurity of IoT devices by documenting best practices for manufacturers. By following the standard, manufacturers can be confident their devices are more resistant to common cyberattacks.

Scope

The standard applies to a broad range of consumer IoT products, including smart TVs, wearables, thermostats, connected appliances, and more. Generally, it is any product that is able to connect to the internet and is not a typical personal computer, tablet, or phone.

1.3.1. Key Provisions of ETSI EN 303 645

ETSI EN 303 645 has 13 high-level recommendations, including:

Password Management

No universal default passwords should be used, and devices should allow users to create strong, unique passwords.

Vulnerability Management

Manufacturers should have a process for handling reported vulnerabilities and issuing security patches in a timely manner.

Software Updates

Devices should be designed to receive software updates for a certain period to address security vulnerabilities and bugs.

Secure Communication

The standard recommends secure communication protocols to protect data transmitted between devices and other systems.

Minimising Attack Surface

The standard encourages manufacturers to minimise the number of entry points for potential attackers by reducing unnecessary features and functionalities.

1.4. What is Raspberry Pi Doing?

As a manufacturer of general-purpose computing products, Raspberry Pi is not directly responsible for ensuring that products meet the requirements of the PSTI and the Product Security and Telecommunications Infrastructure Regulations. Designers who integrate a Raspberry Pi product into their equipment are likely to have to meet the requirements however. Here are some points to consider:

Security Features

Raspberry Pi devices leverage various security features native to the operating system. These features include user authentication, encryption, and firewalls. Designers can configure these features to improve their device's security. For example, designers choosing a Raspberry Pi may wish to use disk encryption to prevent private data from being accessed, or to ensure code executed has not become corrupt or been tampered with. The dm-verity and LUKSv2 technologies are examples of this, respectively. Such features can be used with industry best practices, such as **NIST Special Publication 800-63B**, to ensure that user authentication is robust.

Vulnerability Reporting

Known vulnerabilities can be reported to security@raspberrypi.com. When necessary, information about known vulnerabilities will be published via our **Product Information Portal (PIP)**.

Operating System Updates

Our operating systems continue to be fully backward compatible with even our oldest hardware, meaning our users are always able to take advantage of the latest security updates. The open-source nature of our operating system provides users with herd immunity from security threats, and the system itself benefits from having a huge number of active developers at hand.

Security-Sensitive Security Parameters

The soon-to-be-released Raspberry Pi Signed Boot Provisioner will ensure that only customer-trusted software is installed on any device, enforcing a chain of trust that extends from the bootloader through to the customer application. Designers will have control of this tool to ensure a secure environment during provisioning, and will be able to take absolute control over the software deployed to their devices.

Secure Communication

Raspberry Pi Connect facilitates our “it just works” approach by providing a secure and easy-to-use way to access your Raspberry Pi remotely, from anywhere on the planet, using just a web browser. For devices that require low data rate communication — a common feature of IoT applications — Raspberry Pi enables HTTPS and MQTT with dTLS-encrypted communication protocols.

Raspberry Pi is a trademark of Raspberry Pi Ltd