# IoT Common Security Requirements Guidelines 2021:

# CCDS-GR01-2021

# Ver. 1.0

General Incorporated Association

Connected Consumer Device Security Council

November 24, 2020

Update History

| Revision | Date of Update | Description of Update | Formulated by |
|---|---|---|---|
| Rev. 1.0 | 2020/11/24 | Rev. 1.0 release | CCDS |

■Trademarks

・All company names, product names and the like in this document are either trademarks or registered trademarks of their respective companies.

■Notice

・Information in this document is that available at the time of publication of this document and is subject to change without notice.

・Duplication or reproduction of the contents of this document without prior permission from the CCDS is strictly prohibited.

## 1. Purpose of This Document

This Guidelines defines a minimum set of requirements (action level: ★) to be fulfilled by connected devices. These minimum requirements are to apply to IoT device and system implementations of connected devices.

## 2. Scope of Granting of the CCDS Certification Mark

The scope of granting of the CCDS Certification Mark encompasses those device and system implementations of Internet Protocol-ready hardware and software interfaces.

## 3. Common Requirements

The table below summarizes the common individual requirements.

| . | Target Level | Category of Revision from the 2019 Requirements | Certification Requirement | Kind of Vulnerability | Explanation (Background of the threat and example) |
|---|---|---|---|---|---|
| 1 | ★<br>(Common) | − | There must not be Web input-based SQL injection defects. | CWE-89: SQL injection | [Background of the threat]<br>An inadequately invalidated SQL syntax contained in user input could override security checks or allow statements to be inserted, a backend database to be tampered or system commands to be executed. (CWE-TOP6)<br>[Examples]<br>・Wi-Fi wireless router, (CVE-2015-6319)<br>[Remarks]<br>・Requirements defined in "UK Code of Practice for consumer IoT security"<br>13. Validate input data |
| 2 | ★ | − | There must not | CWE-352: | [Background of the threat] |

| | | | | | |
|---|---|---|---|---|---|
| | (Common) | | be Web input-based cross-site request forgery defects. | Cross-site request forgeries | A vulnerability that arises as a result of failure to verify that user requests are properly formatted. Attackers could fool clients, causing them to transmit unintended requests to a Web server.<br>(CWE-TOP7)<br>[Examples]<br>・Wi-Fi wireless router (CVE-2014-7270)<br>[Remarks]<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>13. Validate input data |
| 3 | ★<br>(Common) | — | There must not be Web input-based path traversal defects. | CWE-22: Path traversal | [Background of the threat]<br>The vulnerability of allowing access to a restricted directory by creating a pathname from external input. (CWE-TOP11)<br>[Examples]<br>・IP camera (CVE-2017-7461)<br>[Remarks]<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>13. Validate input data |
| 4 | ★<br>(Common) | — | TCP/UDP ports out of service must not be left open for use from outside. | CWE-671: Lack of administrator control over security (unnecessary TCP/UDP ports left open) | [Background of the threat]<br>If TCP/UDP ports that are not needed for functional or service purposes are left open, they could open a way communication that might be abused by cyber attackers.<br>[Examples] |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | ・Wi-Fi wireless routers, IP cameras and more<br>[Remarks]<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>6. Minimize exposed attack surfaces |
| 5 | ★<br>(Common) | Modified | Appropriate certification practices (unique IDs and passwords are assigned by device) and communication access control must be in place in the TCP/UDP sessions relevant to system operations. | CWE-287: Inappropriate certification practices (inappropriate access management of TCP/UDP ports) | [Background of the threat]<br>Appropriate certification practices or communication access control is not implemented on the open ports relevant to system operations in the TCP/UDP sessions, threatening problems such as information leaks from the data stored in the devices or privilege elevation (seizure of control over the management functions) can occur.<br>[Examples]<br>・Wi-Fi wireless routers, IP cameras and more<br>[Remarks]<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>6. Minimize exposed attack surfaces |
| 6 | ★<br>(Common) | Modified | ・Certification information must be capable of being re-edited (that is, it is not | CWE-259: Problems associated with a hard-coded password (such as an | [Background of the threat]<br>If certification information used to access a device or application, such as ID or password information, is endangered when it is |

| | | | | | |
|---|---|---|---|---|---|
| | | | hard-coded). | inappropriately implemented or hard-coded access code or unmodifiable access code). | hard-coded or the implementation prohibits its modification, there would be no way responding to it, leading to vulnerabilities.<br>[Examples]<br>・Medical institution systems<br>[Remarks]<br>・Requirements defined in “Certification of Compliance of Devices with the Relevant Security Standards”<br>・Requirements defined in the “California State Laws”<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>1. No Default Password (Certification information must be set before any default password can be used.) |
| 7 | ★<br>(Common) | － | ・Functions must be in place that permit uses to easily delete information defined or collected by them while using a device.<br>・Updated system software must be capable of being maintained even after such | Inadequate implementation of functions allowing for scrapping or reuse.<br>・No applicable CWE | [Background of the threat]<br>If a function that permits deleting security settings, confidential information, privacy information and other information retained by devices or applications is not implemented, such information could leak out upon scrapping or reuse.<br>[Examples]<br>・PCs, USB memory smartphones<br>[Remarks]<br>・Requirements defined in the |

| | | | | | |
|---|---|---|---|---|---|
| | | | information has been deleted. | | “UK Code of Practice for consumer IoT security”<br>8. Ensure that personal data is protected<br>11. Make it easy for consumers to delete personal data |
| 8 | ★<br>(Common) | — | The latest scheme of certification recommended by the Wi-Fi Alliance ® must be supported. | CWE-326: Problems of the absence of an encryption scheme having a strength (latest Wi-Fi communication encryption function not implemented). | [Background of the threat]<br>The scheme of communication encryption used in the Wi-Fi devices is not the latest one but it employs vulnerable encryption protocol or encryption algorithm.<br>[Examples]<br>・Wi-Fi wireless router<br>[Remarks]<br>・Requirements covered din the “UK Code of Practice for consumer IoT security”<br>5. Communicate securely |
| 9 | ★<br>(Common) | Additional requirements | 1) The latest pairing scheme recommended by the Bluetooth SIG must be supported.<br>2) Profiled irrelevant to Bluetooth must not be recognizable.<br>3) Bluetooth devices must be free from Blueborne vulnerabilities. | CWE-287: Inappropriate cortication procedure (Bluetooth pairing function not implemented). | [Background of the threat]<br>1) Specifications earlier than Bluetooth 2.0+EDR would require the devices to be paired with each other to enter a numeric sequence, called a “PIN code.” Typically, implementations involving the entry of a four-digit, such as 0000 are so common that they could be attacked by entering pre-planned sequences, compromising security easily.<br>2) The implementation of unnecessary Bluetooth protocols could open a way for |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | attacks being launched.<br>3) Use of any device with Blueborne vulnerabilities inherent could allow third parties to use the device at their discretion.<br>[Examples]<br>・Devices adhering to specifications earlier than s Bluetooth 2.0+EDR<br>[Remarks]<br>・Requirements defined in the “UK Code of Practice for consumer IoT security”<br>5. Communicate securely |
| 10 | ★<br>(Common) | ― | Unnecessary device classes must be made non-recognizable for system operation purposes. | Use of device classes that do no require USB<br>・No applicable CWE | [Background of the threat]<br>The implementation of unnecessary device classes could open a way for attacks being launched via malware, for example.<br>[Examples]<br>・USB-mounted devices in general<br>[Remarks]<br>・Requirements defined in “UK Code of Practice for consumer IoT security”<br>6. Minimize exposed attack surfaces |
| 11 | ★<br>(Common) | ― | ・Software update must be possible.<br>・The state of software having been updated | Software update function not implemented<br>・No applicable CWE | [Background of the threat]<br>If a function that permits updating software or firmware upon detection of vulnerabilities in them is not implemented, they could be |

| | | | | | |
|---|---|---|---|---|---|
| | | | must be maintained even after the power is turned off. | | exposed to attacks taking advantage of their security holes.<br>[Examples]<br>・Wi-Fi wireless routers, IP cameras and more<br>[Remarks]<br>・Requirements defined in "Certification of Compliance of Devices with the Relevant Security Standards"<br>・Requirements defined the "UK Code of Practice for consumer IoT security"<br>3. Keep software updated<br>9. Make systems resilient to outages |
| 12 | ★<br>(Common) | New | 1) A contact for information on product vulnerabilities must be available and made public.<br>2) A product security update support site must be available. | ・No applicable CWE | [Background]<br>Security standards in effect in and outside Japan targeting IoT devices define an organizational plan or operational scheme for product providers.<br>[Remarks]<br>Requirements defined in NISTIR 8259 "Foundational Cybersecurity Activities for IoT Device Manufactures"<br>Activity 6: Decide what to communicate to customers and how to communicate it. |