TOP 10 CONSUMER IoT CYBERSECURITY VULNERABILITIES IN 2023

1 | Using Default Credentials

When default credentials, such as passwords, are common to all devices in their operational states, it becomes trivial for an attacker to take control of the device.

2 | Incorrect classification of data

Correct classification of collected data (personal identifiable information, telemetry) is needed to comply with country national laws. When data is wrongly processed, it exposes the entity to financial penalties.

3 | Sensitive security parameter stored insecurely

Security-related secret information (cryptographic keys, credentials, etc.) needs to be encrypted when stored. Its exposure can lead to data leaks or unauthorised access to the device.

4 | Software services running as root

Within a device, processes and services should run with the least level of privilege needed. When everything is running as root it facilitates pivoting actions of an attacker.

5 | Insecure communication

Data in transit should be protected according to the risk. Too often critical data is communicated without appropriate protection.

6 | Wrong scope of compliance (ICS "not supported")

Most cybersecurity testing requires documentation to declare the product cybersecurity features. Mistakes on the scope will impact compliance and product security.

7 | Enabled debug interface

UART, JTAG, etc. must be physically and logically disabled or they can provide access to the key device features.

8 | Missing Vulnerability Disclosure Policy

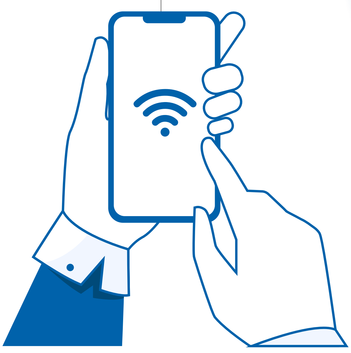
VDP enables a security researcher to contact the manufacturer through a secure point of contact. When this is found missing, the vulnerability disclosure will not be coordinated and can become public before a patch is released.

9 | Undefined minimum support period

Without the support period, the buyer cannot make an informed decision. They don't know when the product will stop receiving security updates and, therefore, may become insecure.

10 | Insecure boot

Secure boot helps make sure that a device boot uses firmware that is trusted by manufacturers. If boots are insecure, attackers can boot the device with a compromised firmware.



Find out more about TÜV SÜD's cybersecurity solutions.
www.tuvsud.com/en-sg/themes/cybersecurity