Action Plan for RED 3(3)(d) & 3(3)(e) Compliance

Introduction

The directives applies for products that will be sold in EU market:

- *EN 18031-1*: Privacy and data protection;
- *EN 18031-2*: Fraud protection (required only for paid based products);

Phase 1: Information and Compliance Analysis

- 8devices will perform internal based audit using Black duck or Emba penetration testing tools for OpenWrt or FirmUx based products, this will accompany the self declared compliance for RED 3(3)d and 3(3)e and provide insight for customers upon request how to achieve or improve their devices security;
- 8devices will share details on how to achieve compliance using standard OpenWrt for existing 8devices SOMs, including mandatory requirements that must be implemented for proprietary customer based OpenWrt versions. This will be provided as general guidelines and best security practices at our external gitlab infrastructure;
- Guidelines will include a secure way of storing customers information of the password, usage of encryption methods, salt methods etc if not already available on their software solution;
- A list of features for OpenWrt that should be disabled or avoided or improved will be provided in the upcoming guidelines (Web/SSH passwords, WPA2 keys, API tokens, Syslogs, connection history, traffic metadata, Wi-Fi management (hostapd) etc);

Phase 2: Map Against EN 18031-1 and EN 18031-2 Requirements

Create a compliance matrix to determine where requirements are satisfied or need action, this will be done for FirmUx and can be used for OpenWrt as guidelines.

Phase 3: Software Hardening & Privacy Protection guidelines

Ensure data collection, storage, and transmission align with privacy principles, the general guidelines how to achieve that using OpenWrt will be provided.

Encrypt all interfaces:

- Force HTTPS with option to disable HTTP;
- Enforce strong SSH settings (Dropbear/OpenSSH) and disable Telnet;
- Use salted password and access for user interfaces;
- Prepare signed firmware build process and guidelines;

Secure firmware updates:

- Enable signed firmware images using OpenWrt using your own key infrastructure (this will provided as separate project on external Gitlab at 8devices infrastructure, later can be migrated to 8devices Github);
- Validate signatures at boot or upgrade (this will be provided firstly as external Gitlab from 8devices, that will provide customers possibility to build their own secure boot version, that is specific to their platform and includes 8devices proprietary secure boot logic);

Prevent unauthorized device access:

- Generate unique device keys on first boot (ECC/RSA) stored securely (typically done on all existing devices, even OpenWrt based);
- Avoid using default hostnames or shared certificates (add option to generate own certificate or upload);
- Integrate sysupgrade OTA (FirmUx only);
- Require a more secure password (length and symbols requirements);

Protect credentials and keys:

- Store Wi-Fi and admin passwords in secure, non-readable config files;
- Salt and hash any stored secrets;

Secure bootloader and image:

- Lock down access to bootloader if applicable (U-Boot password based logic will be built-in the shipped bootloader for all 8devices products);
- Enable image integrity verification (signed image against certificate, this will be added to the general guidelines how the customer can achieve this and have compatibility with his own solution). This might include a paid support effort;

Phase 4: Verification, Documentation, and Support

Testing Against RED 3.3 EN 18031 Standards:

- 8devices will perform general penetration testing using Black duck or Emba solution toolkit as described in previous chapters;

Provide more detailed technical documentation:

- 8devices will demonstrate compliance for notified bodies or market, this will self compliance declaration, upon request penetration report will be provided for FirmUx based products and general guidelines for customers how to achieve RED requirements using OpenWrt (a paid support/subscription service will be required);

Update the technical file to include:

- Software architecture and security diagrams for FirmUx based products will be provided;
- Privacy/data flow chart (FirmUx only);
- References to firmware version(s) covered (packages version used etc, FirmUx only);

Prepare the Self Declaration of Conformity to include:

- RED Art. 3(3)(d) and 3(3)(e);
- Harmonized standards: EN 18031-1, EN 18031-2;
- Display data usage notice in the web UI (privacy-first design, FirmUx only);
- Provide regular secure firmware updates (FirmUx only);
- Include RED compliance information in packaging or web support pages;
- Create a Wiki guidelines for corporate clients;