OWASP Secure Medical Device Deployment Standard: Purchasing Assessment Criteria

Christopher Frenz

Version 1.0 9/12/17

Network Communication Assessment Criteria

Does this device have the ability to connect to a network via an Ethernet connection?

Does this device have the ability to connect to a network via Wi-Fi? If so, what are the WiFi network requirements? Is WiFi optional or required for the device to function?

Does the device support any other networking protocols (e.g. Bluetooth)? If so, please specify. Are these other networking protocols optional or required for the device to function?

What public facing IP addresses (if any) will this device need to communicate with? Will the device act as the client or server for these communications? What ports and protocols are required for these communications?

For any public facing systems data is exchanged with can a SOC2 report or other independent security assessment be provided? If so, please attach.

What internal deployed systems (if any) will this device need to communicate with? Will the device act as the client or server for these communications? What ports and protocols are required for these communications?

Software Assessment Criteria

Is a software manifest available that lists ALL software components used in this device and their corresponding version numbers, including the Operating System and any libraries or other software products (proprietary and open source)? If so, please attach.

Is there a mechanism for updating the software on this device? If so, please describe.

Were secure SDLC principles used in the development of this device?

Were any independent penetration tests or other independent security assessments performed against the device? If so, can the reports and remediations (if any) be shared?

Were Privacy by Design Principles used in the development of this device?

Does this device adhere to the Hippocratic Oath for Connected Medical Devices?

Are their any unpatched US-CERT advisories or any other publicly disclosed vulnerabilities present in any software component used in this device?

How long will the software on this device be supported?

Is there an upgrade path when the installed software goes end of life?

Is there an in place mechanism for vulnerabilities to be disclosed to the manufacturer?

Device Control Assessment Criteria

What type of data does this device collect, process, store and transmit?

Does the device allow for the default credentials to be changed?

Are any hardcoded devices included with the device?

Does the device support account lockout if a threshold of invalid login attempts is exceeded? If so, what is the threshold?

Does the device support encrypting data in transit? If so, how?

Does the device support encrypting data at rest? If so, how?

Does the vendor make available spare copies of the software or firmware for quick restore of a device?

Can the device (including any custom settings) be backed up?

Does the device support different user accounts with varying access levels?

Does the device have a management interface that is distinct from other network interfaces?

Does the device support mechanisms for restricting access to the management interface?

Does the device have logging or other auditing mechanisms in place? If so, can these logs be exported to a syslog or like server?

Is a device hardening guide available? If so, please attach.

Acknowledgements:

Thanks to Shawn Merdinger for inspiring the idea