

SEPTEMBER 26, 2016

1

UL 2900-2-1

Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems

Issue Number: 2

September 26, 2016

Summary of Topics

The second issue of the Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems, UL 2900-2-1, contains revisions to requirements for documentation for product use; safety-related security risk management; known vulnerability testing; malware testing; malformed input testing; software weakness analysis; structured penetration testing; static source code analysis; static binary and bytecode analysis; as well as some editorial revisions.

UL's Outlines of Investigation are copyrighted by UL LLC. Neither a printed nor electronic copy of an Outline of Investigation should be altered in any way. All of UL's Outlines of Investigation and all copyrights, ownerships, and rights regarding those Outlines of Investigation shall remain the sole and exclusive property of UL LLC.

COPYRIGHT © 2016 UL LLC

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM**

Documents
Document Sharing Hub

No Text on This Page



CONTENTS

INTRODUCTION

1 Scope	4
2 Normative References	4
3 Glossary	5

DOCUMENTATION FOR PRODUCT, PROCESSES, AND USE

4 Product Documentation	7
5 Process Documentation	7
6 Documentation for Product Use	7
6.1 Safety-related security considerations for product use	7
6.2 Instructions	7

SECURITY CONTROLS

7 General	8
8 Access Control, User Authentication, and User Authorization	8
9 Remote Communication	8
10 Cryptography	8
11 Product Management	8

PRODUCT ASSESSMENT

12 Safety-Related Security Risk Management	8
12.1 Risk analysis	8
12.2 Risk evaluation	10
12.3 Risk control	10
12.4 Coverage of security analysis and testing	11
13 Known Vulnerability Testing	14
14 Malware Testing	14
15 Malformed Input Testing	14
16 Structured Penetration Testing	15
17 Software Weakness Analysis	16
18 Static Source Code Analysis	16
19 Static Binary and Bytecode Analysis	16

ORGANIZATIONAL ASSESSMENT

20 Lifecycle Security Processes	16
20.1 Quality management processes	16
20.2 General procurement processes	16
20.3 Procurement risk management process	17
20.4 Product update release and patch management process	17
20.5 Decommissioning process	17
20.6 Packaging and shipment	18

INTRODUCTION

NOTE: This Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems, is to be used in conjunction with the Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1. The requirements for network connectable components of healthcare systems are contained in this part 2 outline and UL 2900-1. Requirements of this Part 2 outline, where stated, amend the requirements of UL 2900-1. Where a particular subclause of UL 2900-1 is not mentioned in UL 2900-2-1, the UL 2900-1 subclause applies.

1 Scope

1.1 This security evaluation outline applies to the testing of network connected components of healthcare systems. It applies to, but is not limited to, the following key components:

- a) Medical devices;
- b) Accessories to medical devices;
- c) Medical device data systems;
- d) In vitro diagnostic devices;
- e) Health information technology; and
- f) Wellness devices.

2 Normative References

2.1 The Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, shall be applied as specified in this outline.

2.2 The Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971:2007, shall be applied as specified in this outline.

2.3 The Standard for Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes, ISO 13485:2003, shall be applied as specified in this outline.

2.4 The Standard for Medical Device Software – Software Life Cycle Processes, IEC 62304:2006, shall be applied as specified in this outline.

3 Glossary

3.1 AUTHENTICATION – The process of verifying the identity of an entity.

3.2 AUTHORIZATION – The process of giving an entity permission to access or manipulate the product, or the property that an entity has such permission.

3.3 BYTECODE – Instructions and/or data that are created from source code as an intermediate step before generating binary code. Bytecode is independent of a specific processor architecture and is typically handled by a virtual machine or interpreter.

3.4 COMMON VULNERABILITY SCORING SYSTEM (CVSS) – Specified in ITU-T X.1521, the CVSS is a publicly available resource providing a means for prioritizing vulnerabilities in terms of exploit potential.

3.5 COMMON WEAKNESS SCORING SYSTEM (CWSS) – Specified in ITU-T X.1525, the CWSS is a publicly available resource providing a means for prioritizing CWEs based on their technical impact, ease of attack, and other factors.

3.6 CONFIDENTIALITY – The property that data, information or software is not made available or disclosed to unauthorized individuals, entities, or processes.

3.7 EXPLOIT – An input or action designed to take advantage of a weakness (or multiple weaknesses) and achieve a negative technical impact.

NOTE: The existence of an exploit targeting a weakness is what makes that weakness a vulnerability.

3.8 EXTERNAL INTERFACE – An interface of the product that is designed to potentially allow access to an entity outside the product; for example user interfaces, remote interfaces, local interfaces, wireless interfaces and file inputs.

3.9 FILE – A collection of data or program instructions stored as a unit with a single name.

3.10 INTEGRITY – The property of data, information or software not having been improperly modified.

3.11 KNOWN VULNERABILITY – A vulnerability described in the National Vulnerability Database (NVD).

NOTE: The NVD is accessible at <https://nvd.nist.gov>.

3.12 MALFORMED INPUT TESTING – A black-box testing technique used to reveal software weaknesses and vulnerabilities in a product by triggering them with invalid or unexpected inputs on the external interfaces of the product.

3.13 MALWARE – Software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected systems.

3.14 NETWORK – A collection of nodes and telecommunication links, allowing connected devices, software etc. to exchange data and communicate.

3.15 **PENETRATION TESTING** – A mechanism of evaluation of a product to exploit vulnerabilities and weaknesses discovered in the vulnerability assessment phase.

3.16 **PRODUCT** – The network-connectable device, software or system under test.

3.17 **RISK** – The potential for harm or damage, measured as the combination of the likelihood of occurrence of that harm or damage and the impact of that harm or damage.

3.18 **RISK ANALYSIS** – The systematic use of available information to identify threats and to estimate risk.

3.19 **RISK CONTROL** – Any action taken or feature implemented to reduce risk.

3.20 **RISK MANAGEMENT** – Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk.

3.21 **SECURITY** – The state of having acceptable levels of confidentiality, integrity, authenticity and/or availability of product data and/or functionality.

3.22 **SENSITIVE DATA** – Sensitive data is any critical security parameter that can compromise the use and security of the product such as passwords, keys, seeds for random number generators, authentication data.

3.23 **SOFTWARE** – All pre-loaded data which creates, affects, and/or modifies the functionality of the product. This includes, but is not limited to, firmware, scripts, initialization files, pre-compiled code and interpreted code. This does not include software preloaded and programmed in an IC chip for small functions that require physical access and removal of the IC chip for reprogramming.

3.24 **SOFTWARE WEAKNESS** – A mistake in the architecture, design, coding, build process or configuration of software in the product, that may render the product vulnerable to a security exploit.

3.25 **STATIC ANALYSIS** – A process in which source code, bytecode or binary code is analyzed without executing the code.

3.26 **THREAT** – A potentially successful attack, involving an adversary utilizing specific techniques and resources to take advantage of specific vulnerabilities or lack of risk controls within a product.

3.27 **TRUSTED PLATFORM MODULE** – An international standard that defines the requirements for a dedicated microprocessor with requirements for storage of cryptographic keys used to secure physical products and the software contained.

3.28 **USER** – A person or process using a product or accessing it over one of its external interfaces.

3.29 **VENDOR** – The manufacturer, reseller or supplier of a product, which takes final responsibility for the cybersecurity of that product towards the purchaser and/or user and which submits that product for testing according to this outline.