ANSI/CAN/UL 2900-2-3:2020

JOINT CANADA-UNITED STATES NATIONAL STANDARD

STANDARD FOR SAFETY

Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems

Approved American National Standard
ANSI
ANSI/UL 2900-2-3-2020

Standards Council of Canada
Conseil canadien des normes

SCC FOREWORD

National Standard of Canada

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems, ANSI/CAN/UL 2900-2-3

First Edition, Dated January 31, 2020

Summary of Topics

This First Edition of UL 2900-2-3, Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems, applies to the evaluation of security and life safety signaling system components including, but not limited to, alarm control units; intrusion detection equipment; general purpose signaling units; digital video equipment and systems; mass notification and emergency communication / evacuation equipment and systems; control servers; alarm automation system software; alarm receiving equipment; anti-theft equipment; automated teller machines; fire alarm control systems; network connected locking devices; PSIM systems; smoke control systems; smoke / gas / CO detection devices; audible and visual signaling devices (fire and general signaling); access control equipment and systems; and smart locks.

The requirements are substantially in accordance with Proposal(s) on this subject dated December 21, 2018 and September 13, 2019.

No Text on This Page

ANSI/UL 2900-2-3-2020

JANUARY 31, 2020

ANSI/CAN/UL 2900-2-3:2020

Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems

First Edition

January 31, 2020

This ANSI/CAN/UL Standard consists of the First Edition.

The most recent designation of ANSI/UL 2900-2-3 as an American National Standard (ANSI) occurred on January 31, 2020. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page, Preface or SCC Foreword.

This standard has been designated as a National Standard of Canada (NSC) on January 31, 2020.

No Text on This Page

CONTENTS

APPENDIX D

Preface

This is the First Edition of the ANSI/CAN/UL 2900-2-3, Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems.

UL is accredited by the American National Standards Institute (ANSI) and the Standards Council of Canada (SCC) as a Standards Development Organization (SDO).

This Standard has been developed in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization.

This ANSI/CAN/UL 2900-2-3 Standard is under continuous maintenance, whereby each revision is approved in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization. In the event that no revisions are issued for a period of four years from the date of publication, action to revise, reaffirm, or withdraw the standard shall be initiated.

In Canada, there are two official languages, English and French. All safety warnings must be in French and English. Attention is drawn to the possibility that some Canadian authorities may require additional markings and/or installation instructions to be in both official languages.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at http://csds.ul.com.

To purchase UL Standards, visit the UL Standards Sales Site at http://www.shopulstandards.com/HowToOrder.aspx or call tollfree 1-888-853-3503.

This Edition of the Standard has been formally approved by the UL Standards Technical Panel (STP) on Software Cybersecurity for Security and Life Safety Signaling Systems, STP 2900-2-3.

This list represents the STP 2900-2-3 membership when the final text in this standard was balloted. Since that time, changes in the membership may have occurred.

STP 2900-2-3 Membership

Name	Representing	Interest Category	Region
Ahmadi, Mike	M. Ahmadi	General	USA
Barker, David	Stanley Black & Decker	Producer	USA
Baroncini, Vincent	Siemens Industry Inc	Producer	USA
Biggs, Douglas	UL LLC	Testing and Standards	USA
Chevalier, Mathieu	Genetec	Producer	Quebec, Canada
Cosman, Eric	OIT Concepts LLC	Non-voting	USA
Curtis, Bill	Consortium for IT Software Quality (CISQ)	Testing and Standards	USA

STP 2900-2-3 Membership Continued on Next Page

STP 2900-2-3 Membership Continued

Name	Representing	Interest Category	Region
Davis, Barbara	Underwriters Laboratories, Inc.	STP Project Manager – Non-voting	USA
Dawson, Joe	EWA-Canada (an INTERTEK Co)	Testing and Standards	Newfoundland, Canada
Garvy, Patrick	Honeywell	Producer	USA
Greko, Joshua	Dice Corp	Producer	USA
Griffith, Steve	NEMA	Non-voting	USA
Hoskins, Bryan	Oklahoma State University	General	USA
Lanning, Andrew	Intetrated Security Technologies	Supply Chain	USA
Lattman, Douglas	United Technologies Corp	Producer	USA
Lee, Douglas	US Consumer Product Safety Commission	Non-voting	USA
Li, Xiaodong	Lenovo (Beijing) LTD	Producer	China
Martin, Robert	MITRE Corp	Commercial/Industrial User	USA
Mendoza, Ernesto	Signify North America Corporation	Commercial/Industrial User	USA
Milke, James	University of Maryland	General	USA
Newsome, Leon	EATON	Producer	USA
Niati, Raheleh	Microm Technologies Ltd	Producer	Ontario, Canda
Prince, Deborah	Underwriters Laboratories Inc.	STP Chair – Non-voting	USA
Redwood, William	Nebraska Applied Research Institute	Supply Chain	USA
Rowland, Michael	IAEA	Government	Austria
Salveggio, Eric	MSAG	General	USA
Shkolnik, Moti	Firedome	Supply Chain	USA
Tan, Simin	CASC	Testing and Standards	China
Thayer, Rodney	Smithee Solutions LLC	General	USA
Toika, Michael	Addison Fire Protection District #1	AHJ	USA
Tran Phat	BC Safety Authority	Non-voting	British Columbia, Canada
Vasserman, Eugene	Kansas State University	General	USA
Wang, Hui	CNCERT/CC	General	China
Wright, George	Circadence	General	USA
Wylie, Doug	Sans Institute	General	USA
Wyman, Richard	CS 7 Consulting	General	USA

International Classification for Standards (ICS): 35.030, 35.110, 35.240.50, 35.240.80

For further information on UL standards, please contact:

Underwriters Laboratories Inc.
171 Nepean Street, Suite 400
Ottawa, Ontario K2P 0B4
Phone: 1-613.755.2729

E-mail: ULCStandards@ul.com
Web site: ul.org

This Standard is intended to be used for conformity assessment.

The intended primary application of this standard is stated in its scope. It is important to note that it remains the responsibility of the user of the standard to judge its suitability for this particular application.

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

No Text on This Page

INTRODUCTION

Note: This Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems refers to the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

1 Scope

1.1 This security evaluation standard applies to the evaluation of security and life safety signaling system components. It applies to, but is not limited to, the following products:

a) Alarm Control Units;

b) Network-Based Intrusion Detection System;

c) General Purpose Signaling Units;

d) Digital Video Equipment and Systems;

e) Mass Notification and Emergency Communication / Evacuation Equipment and Systems;

f) Control servers;

g) Alarm Automation System Software;

h) Alarm Receiving Equipment;

i) Anti-Theft Equipment;

j) Automated Teller Machines;

k) Fire Alarm Control Systems;

l) Network Connected Locking Devices;

m) Physical Security Information Management (PSIM) Systems;

n) Smoke Control Systems;

o) Smoke / Gas / CO Detection Devices;

p) Audible and Visual Signaling Devices (fire and general signaling);

q) Access Control Equipment and Systems; and

r) Smart Locks.

1.2 This standard does not contain general requirements that are intended to address functional testing of the product unless expressly specified.

1.3 This standard also describes requirements for the product risk management process carried out by the vendor of the product, including a list of security controls that the product (or the vendor, as applicable) shall comply with unless a risk assessment done by the vendor shows that the risk of not implementing one of these security controls is acceptable.

2 Normative References

2.1 All references are for the current published version of the document unless stated otherwise.

Normative References are included in Section 2 of the Standard for Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

3 Glossary

Glossary Terms are included in Section 3 of the Standard for Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

4 General

4.1 This standard includes three levels of security requirements that are applicable to the product with an increasing level of security for higher levels. The levels and their description are defined in Table 4.1.

Table 4.1

Level	Description
L1	Includes foundational cybersecurity testing requirements for security risk assessment of software in products covered in this standard. Provides assessment of general security capabilities of a product with limited knowledge of the internal security controls of the product. L1 does not require the submission of source code. This level is closest to “black box” testing. L1 is recommended as a minimum level of assessment.
L2	Includes L1 assessment and testing requirements and additional supplemental requirements for security risks assessment of software in products. Source code is tested at this level. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product. Because specific protections for sensitive data are included at L2, this is the lowest level recommended for products sending, receiving, or processing sensitive data.
L3	Includes L1 and L2 assessment and testing requirements and additional supplemental requirements of the vendor process and management. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product and knowledge of the business practices of the vendor to support the lifecycle of the product.

4.2 The product shall comply with the clauses identified in the tables of each section of this standard per the Level intended. The level intended will be marked with an X per the applicable clause. Where an X is not applied, the clause is not mandatory for the Level. In keeping with this approach, when a clause calls for compliance with another section of this standard, only sub-clauses for the level intended (marked with an “X”) are applicable.

DOCUMENTATION OF PRODUCT, PRODUCT DESIGN AND PRODUCT USE

5 Product Documentation

Table 5.1

Clause		L1	L2	L3
5.1	The product shall comply with: Product Documentation, Section 4.1.1 (c), (d), (e) and (f) of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
5.2	The product shall comply with: Product Documentation, Section 4.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
5.3	The product shall comply with: Product Documentation, Section 4.1.1(b) of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

6 Product Design Documentation

Table 6.1

Clause		L1	L2	L3
6.1	The product shall comply with: Product Design Documentation, Section 5.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

7 Documentation for Product Use

Table 7.1

Clause		L1	L2	L3
7.1	The product shall comply with: Documentation for Product Use, Section 6.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.2	The product shall comply with: Documentation for Product Use, Section 6.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.3	The product shall comply with: Documentation for Product Use, Section 6.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.4	The product shall comply with: Documentation for Product Use, Section 6.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

Table 7.1 Continued on Next Page

Table 7.1 Continued

Clause		L1	L2	L3
7.5	The product shall comply with: Documentation for Product Use, Section 6.5 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.6	The product shall comply with: Documentation for Product Use, Section 6.6 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.7	The product shall comply with: Documentation for Product Use, Section 6.7 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.8	The product shall comply with: Documentation for Product Use, Section 6.8 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.9	The product shall comply with: Documentation for Product Use, Section 6.9 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.10	The product shall comply with: Documentation for Product Use, Section 6.10 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

RISK CONTROLS

8 General

Table 8.1

Clause		L1	L2	L3
8.1	The product (or the product's vendor, as applicable) shall comply with all of the applicable controls specified in Clauses 9 – 12 of this standard, unless the risk assessment performed by the vendor according to Section 13, Vendor Product Risk Management Process, shows that the risks associated with not implementing a specific control are acceptable in product use.	X		
8.2	The product shall comply with: Risk Controls – General, Section 7.1.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
8.3	The product shall comply with: Risk Controls – General, Section 7.1.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

9 Access Control, User Authentication and User Authorization

Table 9.1

Clause		L1	L2	L3
9.1	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.2	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.3	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.4	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.5	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.5 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.6	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.6 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.7	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.7 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.8	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.8 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
9.9	The product shall comply with: Access Control, User Authentication and User Authorization, Section 8.9 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

10 Remote Communication

Table 10.1

Clause		L1	L2	L3
10.1	The product shall comply with: Remote Communication, Section 9.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

11 Sensitive Data

Table 11.1

Clause		L1	L2	L3
11.1	The product shall comply with: Sensitive Data, Section 10.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
11.2	The product shall comply with: Sensitive Data, Section 10.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
11.3	The product shall comply with: Sensitive Data, Section 10.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
11.4	The product shall comply with: Sensitive Data, Section 10.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

12 Product Management

Table 12.1

Clause		L1	L2	L3
12.1	The product shall comply with: Product Management, Section 11.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.2	The product shall comply with: Product Management, Section 11.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.3	The product shall comply with: Product Management, Section 11.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.4	The product shall comply with: Product Management, Section 11.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.5	The product shall comply with: Product Management, Section 11.5 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.6	The product shall comply with: Product Management, Section 11.6 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
12.7	The product shall comply with: Product Management, Section 11.7 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
12.8	The product shall comply with: Product Management, Section 11.8 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

RISK MANAGEMENT

13 Vendor Product Risk Management Process

Table 13.1

Clause		L1	L2	L3
13.1	The product shall comply with: Vender Product Risk Management Process, Section 12.1 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
13.2	The product shall comply with: Vender Product Risk Management Process, Section 12.2 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
13.3	The product shall comply with: Vender Product Risk Management Process, Section 12.3 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
13.4	The product shall comply with: Vender Product Risk Management Process, Section 12.4 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
13.5	The product shall comply with: Vender Product Risk Management Process, Section 12.5 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
13.6	The product shall comply with: Vender Product Risk Management Process, Section 12.6 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
13.7	The product shall comply with: Vender Product Risk Management Process, Section 12.7 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
13.8	The product shall comply with: Vender Product Risk Management Process, Section 12.8 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	

VULNERABILITIES AND EXPLOITS

14 Known Vulnerability Testing

Table 14.1

Clause		L1	L2	L3
14.1	The product shall comply with: Known Vulnerability Testing, Section 13.1 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
14.2	The product shall comply with: Known Vulnerability Testing, Section 13.2 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	

15 Malware Testing

Table 15.1

Clause		L1	L2	L3
15.1	The product shall comply with: Malware Testing, Section 14.1 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
15.2	The product shall comply with: Malware Testing, Section 14.2 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	

16 Malformed Input Protocol Testing (also reference Appendix D)

Table 16.1

Clause		L1	L2	L3
16.1	The product shall comply with: Malformed Input Testing, Section 15.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.2	The product shall comply with: Malformed Input Testing, Section 15.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.3	The product shall comply with: Malformed Input Testing, Section 15.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.4	The product shall comply with: Malformed Input Testing, Section 15.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.5	The product shall comply with: Malformed Input Testing, Section 15.5 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.6	The product shall comply with: Malformed Input Testing, Section 15.6 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.7	The product shall comply with: Malformed Input Testing, Section 15.7 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.8	The product shall comply with: Malformed Input Testing, Section 15.8 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.9	The product shall comply with: Malformed Input Testing, Section 15.9 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

Table 16.1 Continued on Next Page

Table 16.1 Continued

Clause		L1	L2	L3
16.10	The product shall comply with: Malformed Input Testing, Section 15.10 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
16.11	The product shall comply with: Malformed Input Testing, Section 15.11 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

17 Structured Penetration Testing

Table 17.1

Clause		L1	L2	L3
17.1	The product shall comply with: Structured Penetration Testing, Section 16.1 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
17.2	The product shall comply with: Structured Penetration Testing, Section 16.2 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
17.3	The product shall comply with: Structured Penetration Testing, Section 16.3 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		
17.4	The product shall comply with: Structured Penetration Testing, Section 16.4 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.	X		

SOFTWARE WEAKNESS ANALYSIS

18 Software Weakness Analysis

Table 18.1

Clause		L1	L2	L3
18.1	The product shall comply with: Software Weakness Analysis, Section 17.1 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	
18.2	The product shall comply with: Software Weakness Analysis, Section 17.2 of the Standard for Software Cybersecurity for Network-Connectable Devices: General Requirements, UL 2900-1.		X	