



JOINT CANADA-UNITED STATES
NATIONAL STANDARD

STANDARD FOR SAFETY

ANSI/CAN/UL 2900-1:2017, Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements



ANSI/UL 2900-1-2017



Standards Council of Canada
Conseil canadien des normes

UL COPYRIGHTED MATERIAL –

NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents

Document Sharing Hub

SCC FOREWORD

National Standard of Canada

A National Standard of Canada is a standard developed by an SCC-accredited Standards Development Organization (SDO), and approved by the Standards Council of Canada (SCC), in accordance with SCC's *Requirements and Guidance-Accreditation for Standards Development Organizations*, and *Requirements and Guidance-Approval of National Standards of Canada Designation*. More information on National Standard requirements can be found at www.scc.ca. An SCC-approved standard reflects the consensus of a number of experts whose collective interests provide, to the greatest practicable extent, a balance of representation of affected stakeholders. National Standards of Canada are intended to make a significant and timely contribution to the Canadian interest.

SCC is a Crown corporation within the portfolio of Industry 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.

Users should always obtain the latest edition of a National Standard of Canada from the standards development organization responsible for its publication, as these documents are subject to periodic review.

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



Documents

Document Sharing Hub

UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1

First Edition, Dated July 5, 2017

Summary of Topics

This First Edition of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, ANSI/CAN/UL 2900-1, has been formally approved by the UL Standards Technical Panel (STP) 2900 on Software Cybersecurity for Network-Connectable Products.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without prior permission of UL.

UL provides this Standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

In no event will UL be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this Standard, even if UL or an authorized UL representative has been advised of the possibility of such damage. In no event shall UL's liability for any damage ever exceed the price paid for this Standard, regardless of the form of the claim.

Users of the electronic versions of UL's Standards for Safety agree to defend, indemnify, and hold UL harmless from and against any loss, expense, liability, damage, claim, or judgment (including reasonable attorney's fees) resulting from any error or deviation introduced while purchaser is storing an electronic Standard on the purchaser's computer system.

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



Documents

Document Sharing Hub

No Text on This Page

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



Documents

Document Sharing Hub



ANSI/UL 2900-1-2017



Standards Council of Canada
Conseil canadien des normes

JULY 5, 2017

1

ANSI/CAN/UL 2900-1

Standard for Software Cybersecurity for Network-Connectable Products,

Part 1: General Requirements

First Edition

July 5, 2017

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

The most recent designation of ANSI/UL 2900-1 as an American National Standard (ANSI) occurred on July 5, 2017. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page, Preface or SCC Foreword.

This standard has been approved as a National Standard of Canada (NSC) by the Standards Council of Canada (SCC).

COPYRIGHT © 2017 UNDERWRITERS LABORATORIES INC.

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



Documents
Document Sharing Hub

No Text on This Page



CONTENTS

Preface	4
---------------	---

INTRODUCTION

1 Scope	4C
2 Normative References	4C
3 Glossary	6
4 Documentation Of Product, Product Design And Product Use	10
4.1 Product Documentation	10
5 Product Design Documentation	11
6 Documentation for Product Use	11
7 Risk Controls	12
7.1 General	12
8 Access Control, User Authentication and User Authorization	12
9 Remote Communication	14
10 Sensitive Data	14
11 Product Management	15

RISK MANAGEMENT

12 Vendor Product Risk Management Process	16
---	----

VULNERABILITIES AND EXPLOITS

13 Known Vulnerability Testing	18
14 Malware Testing	18
15 Malformed Input Testing	18
16 Structured Penetration Testing	20

SOFTWARE WEAKNESSES

17 Software Weakness Analysis	20
18 Static Source Code Analysis	21
19 Static Binary and Bytecode Analysis	21

APPENDIX A (INFORMATIVE)

A1 Sources for Software Weaknesses	A1
--	----

APPENDIX B (INFORMATIVE)

B1 Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable Information	B1
--	----

APPENDIX C (INFORMATIVE)

C1 Requirements for Security Functions	C1
--	----

Preface

This is the First Edition of the ANSI/CAN/UL 2900-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements,.

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

This ANSI/CAN/UL 2900-1 Standard for Safety is under continuous maintenance, whereby each revision is ANSI/CAN approved upon publication. If no revisions occur, the initiation of the review of this Standard will commence within 5 years of the date of publication.

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.

Only metric SI units of measurement are used in this Standard. If a value for measurement is followed by a value in other units in parentheses, the second value may be approximate. The first stated value is the requirement.

Appendices A, B and C, identified as informative, are for guidance and informational purposes only.

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>.

UL's Standards for Safety are copyrighted by UL. Neither a printed nor electronic copy of a Standard should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of UL.

To purchase UL Standards, visit Comm 2000 at http://www.comm-2000.com/help/how_to_order.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 2900, Software Cybersecurity for Network-Connectable Products, STP 2900.

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

STP 2900 Membership

Name	Representing	Interest Category*	Region
Banavara, Harsha	Schneider Electric	Producer	USA
Chevalier, Mathieu	Genetec	Producer	Canada
Costello, Brian	Mitsubishi Electric US	Producer	USA
Cousin, Dmitry	NIST	Government	USA
Datko, Joshua	Cryptotronix	General	USA
Davis, Valara	Underwriters Laboratories, Inc.	STP Project Manager - Non-voting	USA
Douglas, Ahmad	Comcast	Producer	USA
Fisher, Joseph	Affinity IT Security	General	USA
Fitzgerald, Brian	Food & Drug Administration	Government	USA
Gallagher, Lori	Utilities Standards Forum	Commercial/Industrial User	Canada
Goldman, Julian	Massachusetts General Hospital/Partners	Commercial/Industrial User	USA
Haithcock, Diane	Underwriters Laboratories, Inc.	STP Chair - Non-Voting	USA
Harvey, Roy	Osram	Producer	USA
Hertel, Morgan	Rapid Response Monitoring, Inc.	Commercial/Industrial User	USA
Jarzombek, Joe	Synopsys	General	USA
Liang, Steven	BC Safety Authority	General	British Columbia, Canada
Lin, Hikohiro	Panasonic	Producer	Japan
Martin, Robert	MITRE Corp	Government	USA
Mendoza, Ernesto	Advance	Producer	USA
Modeste, Kenneth	UL, LLC.	Testing and Standards	USA
Rowland, Michael	IAEA	General	Austria
Strand, John	BHIS	General	USA
Vasserman, Eugene	Kansas State University	General	USA
Wagoner, Larry	NSA	Government	USA
Wright, George	Georgia Tech Research Institute	General	USA
Wyman, Richard	Idaho National Laboratory	Government	USA
Zanetti, Davide	ABB Switzerland Ltd	Producer	Switzerland

* Testing and Standards interest category is non-voting for SCC.

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

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: customerservice@ulc.ca
Web site: ul.com

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

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



Documents
Document Sharing Hub

INTRODUCTION

1 Scope

1.1 This standard applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware.

1.2 This standard describes:

- a) Requirements regarding the software developer (vendor or other supply chain member) risk management process for their product.
- b) Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware.
- c) Requirements regarding the presence of security risk controls in the architecture and design of a product.

1.3 This standard does not contain requirements regarding functional testing of a product. This means this standard contains no requirements to verify that the product functions as designed.

1.4 This standard does not contain requirements regarding the hardware contained in a product.

2 Normative References

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

[1] *Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems*,
UL 2900-2-1

[2] *Standard for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems*,
UL 2900-2-2

[3] *Standard for Test Access Port and Boundary-Scan Architecture*,
IEEE 1149

[4] *Cybersecurity information exchange – Vulnerability/state exchange – Common vulnerabilities and exposures (CVE)*; retrievable from <https://cve.mitre.org/>,
ITU-T X.1520

[5] *Cybersecurity information exchange – Vulnerability/state exchange – Common vulnerability scoring system (CVSS)*; retrievable from <https://nvd.nist.gov/vuln-metrics/cvss>,
ITU-T X.1521

[6] *Cybersecurity information exchange – Vulnerability/state exchange – Common weakness enumeration (CWE)*,
ITU-T X.1524

[7] Cybersecurity information exchange – Vulnerability/state exchange – Common weakness scoring system (CWSS); retrievable from <https://cwe.mitre.org/cwss>, ITU-T X.1525

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



Documents
Document Sharing Hub