INTERNATIONAL STANDARD

ISO/IEC 18180

First edition
2013-06-15

Information technology — Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2

Technologies de l'information — Spécification de XCCDF (Extensible Configuration Checklist Description Format) version 1.2

Reference number
ISO/IEC 18180:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18180 was prepared by the U.S. National Institute of Standards and Technology (as NIST IR 7275, Revision 4) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by the national bodies of ISO and IEC.

National Institute of
Standards and Technology

U.S. Department of Commerce

NIST Interagency Report 7275
Revision 4

Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2

David Waltermire
Charles Schmidt
Karen Scarfone
Neal Ziring

NIST Interagency Report 7275
Revision 4

Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2

David Waltermire
Charles Schmidt
Karen Scarfone
Neal Ziring

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2011

U.S. Department of Commerce

Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7275 Revision 4
80 pages (Sep. 2011)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgments

The authors of this report, David Waltermire of the National Institute of Standards and Technology (NIST), Charles Schmidt of The MITRE Corporation, Karen Scarfone of Scarfone Cybersecurity, and Neal Ziring of the National Security Agency (NSA), wish to thank all contributors to this revision of the publication, particularly Adam Halbardier of Booz Allen Hamilton, Vladimir Giszpenc, Kent Landfield and Richard Whitehurst of McAfee, Lisa Nordman of The MITRE Corporation, Joe Wolfkiel of DISA, and Shane Shaffer and Matt Kerr of G2, Inc.

The authors would also like to acknowledge the following individuals who contributed to the initial definition and development of the Extensible Configuration Checklist Description Format (XCCDF): David Proulx, Mike Michnikov, Andrew Buttner, Todd Wittbold, Adam Compton, George Jones, Chris Calabrese, John Banghart, Murugiah Souppaya, John Wack, Trent Pitsenbarger, and Robert Stafford. Stephen D. Quinn, Peter Mell, and Matthew Wojcik contributed to Revisions 1, 2, and 3 of this report. Ryan Wilson of Georgia Institute of Technology also made substantial contributions. Thanks also go to the Defense Information Systems Agency (DISA) Field Security Office (FSO) Vulnerability Management System (VMS)/Gold Disk team for extensive review and many suggestions.

Abstract

This report specifies the data model and Extensible Markup Language (XML) representation for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2. An XCCDF document is a structured collection of security configuration rules for some set of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and scoring. The specification also defines a data model and format for storing results of security guidance or checklist testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists and other configuration guidance, and thereby foster more widespread application of good security practices.

Audience

The primary audience of the XCCDF specification is government and industry security analysts, and security management product developers.

Trademark Information

All names are registered trademarks or trademarks of their respective companies.

Contents

Tables

Figures

1. Introduction

1.1 Purpose and Scope

This report defines the specification for the Extensible Configuration Checklist Description Format (XCCDF) version 1.2. The report also defines and explains the requirements that XCCDF 1.2 documents and products (i.e., software) must meet to claim conformance with the specification. This report only applies to XCCDF version 1.2. All other versions are outside the scope of this report.

1.2 Document Structure

The remainder of this report is composed of the following sections and appendices:

- Section 2 provides a list of normative references for the report.
- Section 3 defines selected terms and abbreviations used in the report.
- Section 4 provides the high-level requirements for claiming conformance with the XCCDF version 1.2 specification.
- Section 5 gives an overview of XCCDF and its capabilities.
- Section 6 provides an introduction to the XCCDF data model and details additional requirements and recommendations for XCCDF's use.
- Section 7 discusses XCCDF processing requirements and recommendations.
- Appendix A explains how to convert XCCDF 1.1.4-specific properties to their XCCDF 1.2 counterparts.
- Appendix B provides a change log that documents significant changes to released drafts of this specification. This includes a section-by-section mapping of how the document was reorganized from the previous drafts to this draft. Readers who are familiar with any previous XCCDF versions may find it helpful to review Appendix B first before the rest of the document.

1.3 Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Request for Comment (RFC) 2119 [RFC2119].

Namespace prefixes used in this specification are listed in Table 1.

Table 1: Conventional XML Mappings

Prefix	Namespace	Schema
cpe2	http://cpe.mitre.org/language/2.0	Common Platform Enumeration (CPE) 2.3 Applicability Language
cpe2-dict	http://cpe.mitre.org/dictionary/2.0	CPE 2.3 Dictionary
dc	http://purl.org/dc/elements/1.1/	Simple Dublin Core elements
dsig	http://www.w3.org/2000/09/xmldsig#	Interoperable XML digital signatures
xccdf	http://checklists.nist.gov/xccdf/1.2	XCCDF policy documents
xml	http://www.w3.org/XML/1998/namespace	Common XML attributes
xsd	http://www.w3.org/2001/XMLSchema	XML Schema
xsi	http://www.w3.org/2001/XMLSchema-Instance	XML Schema Instance

2. Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[DCES], DCMI (Dublin Core Metadata Initiative), *Dublin Core Metadata Element Set, Version 1.1*, October 2010, available at <http://dublincore.org/documents/dces/>

[DCXML], DCMI, *Guidelines for Implementing Dublin Core in XML*, April 2003, available at <http://dublincore.org/documents/dc-xml-guidelines/>

[ILSR], IANA, *IANA Language Subtag Registry (ILSR)*, available at <http://www.iana.org/assignments/language-subtag-registry>

[IR7693], NIST, NIST IR 7693, *Specification for Asset Identification 1.1*, June 2011, available at <http://csrc.nist.gov/publications/PubsNISTIRs.html>

[IR7695], NIST, NIST IR 7695, *Common Platform Enumeration: Naming Specification Version 2.3*, August 2011, available at <http://csrc.nist.gov/publications/PubsNISTIRs.html>

[IR7698], NIST, NIST IR 7698, *Common Platform Enumeration: Applicability Language Specification Version 2.3*, August 2011, available at <http://csrc.nist.gov/publications/PubsNISTIRs.html>

[PCRE], Perl Compatible Regular Expressions (PCRE), available at <http://www.pcre.org>

[RFC2119], IETF, RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997, available at <http://www.ietf.org/rfc/rfc2119.txt>

[RFC5646], IETF, RFC 5646, *Tags for Identifying Languages*, September 2009, available at <http://www.ietf.org/rfc/rfc5646.txt>

[UNICODE], Unicode Technical Recommendation No. 18, *Unicode Regular Expressions*, version 9, January 2004, available at <http://unicode.org/reports/tr18/>

[XHTML], W3C (World Wide Web Consortium), *XHTML Basic*, December 2000, available at <http://www.w3.org/TR/2000/REC-xhtml-basic-20001219/>

[XINCLUDE], W3C, *XML Inclusions (XInclude) Version 1.0 (Second Edition)*, November 2006, available at <http://www.w3.org/TR/xinclude/>

[XMLDSIG], W3C, *XML Signature Syntax and Processing (Second Edition)*, June 2008, available at <http://www.w3.org/TR/xmldsig-core/>

[XMLNAME], W3C, *Namespaces in XML 1.0 (Third Edition)*, December 2009, available at <http://www.w3.org/TR/REC-xml-names/>

[XMLSCHEMA], W3C, *XML Schema Part 2: Datatypes Second Edition*, October 2004, available at <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>

[XPATH], W3C, *XML Path Language (XPath) Version 1.0*, November 1999, available at <http://www.w3.org/TR/xpath/>