Network Working Group B. Munyan
Internet-Draft A. Montville
Intended status: Informational Center for Internet Security
Expires: January 16, 2019 S. Banghart
NIST
July 15, 2018

Definition of the ROLIE configuration checklist Extension
draft-mandm-sacm-rolie-configuration-checklist-01

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core by defining a new information-type to ROLIE's atom:category pertaining to security configuration checklists. Additional supporting requirements are also defined which describe the use of specific formats and link relations pertaining to the new information-type.

Status of This Memo

This Internet-Draft will expire on January 16, 2019.

Copyright Notice

Table of Contents

1. Introduction

This document defines an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] protocol [RFC8322] to support the publication of configuration checklist information. Many enterprises operate according to guidance provided to them by a control framework ([CIS_Critical_Controls] , [PCI_DSS] , [NIST_800-53] etc.), which often prescribe that an enterprise define a standard, secure configuration for each technology they operate. Such standard secure configurations are often referred to as configuration checklists. These configuration checklists contain a set of configuration recommendations for a given endpoint. A configuration recommendation prescribes expected values pertaining to one or more discrete endpoint attributes.

2. Terminology

Configuration Checklist A configuration checklist is an organized collection of rules about a particular kind of system or platform.

Configuration Item Generally synonymous with endpoint attribute.

Configuration Recommendation A configuration recommendation is an expression of the desired posture of one or more configuration items. A configuration recommendation generally includes the description of the recommendation, a rationale statement, and the expected state of collected posture information.

TODO: Others?? TBD

TODO: There needs to be a "normative" reference to the SCAP 1.2/3 specifications and schema definitions

3. The 'configuration-checklist' information type

This document defines and registers a new information-type: "configuration-checklist".

The "configuration-checklist" information type represents a body of information describing a set of configuration recommendations. A configuration recommendation is, minimally, a configurable item paired with a recommended value or range of value. Depending on the source, a configuration recommendation may carry with it additional information (i.e. description, references, rationale, etc.). Provided below is a non-exhaustive list of information that may be considered as components of a configuration checklist.

- A "Data Stream":
- A "Benchmark"
- A "Profile"
- A "Value"
- A "Rule" or "Group" of Rules
  - Description
  - Rationale
  - Remediation Instructions
  - Information, described in the dialect of a supported "check system", indicating the method(s) used to audit the checklist configuration item.
- Applicable Platform Information
- Information regarding a set of patches to be evaluated

- Any supported "tailoring" information, providing a method for evaluating entities to refine the recommendations in the data stream without modifying the published data stream content. (WKM NOTE: Does "tailoring" need to be here? Why would any tailoring be included in a published feed? Unless the organization is re-publishing the content with their tailoring included.)

4. Data format requirements

This section defines usage guidance and additional requirements related to data formats above and beyond those specified in [RFC8322] . The following formats are expected to be commonly used to express software descriptor information. For this reason, this document specifies additional requirements to ensure interoperability.

TODO, integrate this information:

- scap-1.2

- PDF

- xccdf-1.2-collection

- oval

- cvrf

- cve (should we reuse the enumref?); Look at the "enumref" and see if we can copy/paste configuration checklist-specific information in a similar manner? Can we then include that enum reference in the ROLIE extension document or should we create a new "enumref" document separately?

- vulnerability

4.1. Data Format 1

4.1.1. Description

This is data section 1 TODO

4.1.2. Requirements

This is requirement 1 TODO

5. rolie:property Extensions

This document provides new registrations for valid rolie:property names. These properties provide optional exposure point for valuable information in the linked content document. Exposing this information in a rolie:property element means that clients do not need to download the linked document to determine if it contains information they are interested in.

A breadth of metadata may be included with a configuration checklist as identifying information. A publishing organization may wish to recognize or attribute checklist authors or contributors, or maintain a revision/version history over time. Other metadata that may be included could indicate the various categories of products to which the checklist applies, such as Operating System, Network Device, or Application Server.

The following list describes various 'rolie:property' constructs.

- contributor (0..n)

  - An unbounded number of "rolie:property" elements with a "name" attribute of "contributor" may be included to indicate those individuals noted as recognized contributors to the configuration checklist and/or the recommendations contained within.

- checklist version: The "value" of the "checklist version" property indicates the version number of the configuration checklist, such as "3.1.1"

- title: The "value" of the "title" property indicates the document title of the configuration checklist, such as "CIS Benchmark for Microsoft Windows Server 2012 R2"

- overview

6. Use of the atom:link element

The following link relations are defined in the following table. These relations are not registered in the Link Relation IANA table due to their niche usage. These link relations are valid for any link element in a checklist Entry.

Name	Description
ancestor	Links to a configuration checklist supersceded by that described in this entry
target-platform	Links to a software descriptor resource defining the software subject to this configuration checklist entry
version	Links to a text resource indicating the version of the configuration checklist

7. Use of atom:category

This document registers an additional atom:category name: 'urn:ietf:params:rolie:category:checklist:nistncpproductcategory'

When the name attribute of a category element is this names, the value attribute SHOULD be one of the valid product categories from the NIST NCP Product Category List, such as:

- Antivirus Software

- Application Server

- Auditing

- Authentication

- Automation/Productivity Application Suite

- Client and Server Encryption

- Configuration Management Software

- Database Management System

- Desktop Application

- Desktop Client

- DHCP Server

- Directory Service

- DNS Server

- Email Server
- Encryption Software
- Enterprise Application
- File Encryption
- Firewall
- Firmware
- Handheld Device
- Identity Management
- Intrusion Detection System
- KVM
- Mail Server
- Malware
- Mobile Solution
- Monitoring
- Multi-Functional Peripheral
- Network Router
- Network Switch
- Office Suite
- Operating System
- Peripheral Device
- Security Server
- Server
- Virtual Machine
- Virtualization Software

- Web Browser

- Web Server

- Wireless Email

- Wireless Network

8. IANA Considerations

Per this document, IANA has added an entry to the "ROLIE Security Resource Information Type Sub-Registry" registry located at https://www.iana.org/assignments/rolie/category/information-type [1].

name: configuration-checklist

index: TBD

reference: This document, Section TODO

TODO add Propertyies and Categories

9. Security Considerations

Any user of this extension should be familiar with the security considerations of ROLIE [RFC8322].

10. Privacy Considerations

Any user of this extension should be familiar with the privacy considerations of ROLIE [RFC8322].

11. References

11.1. Normative References

[RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange (ROLIE)", RFC 8322, DOI 10.17487/RFC8322, February 2018, <https://www.rfc-editor.org/info/rfc8322>.

11.2. Informative References

[CIS_Critical_Controls] "CIS Critical Security Controls", August 2016, <https://www.cisecurity.org/critical-controls/>.

[NIST_800-53]
Hanson, R., "NIST 800-53", September 2007, <http://deusty.blogspot.com/2007/09/stunt-out-of-band-channels.html>.

[PCI_DSS] "PCI Data Security Standard", April 2016, <https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss>.

11.3. URIs

[1] https://www.iana.org/assignments/rolie/category/information-type

Authors' Addresses

Bill Munyan
Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
USA

Email: bill.munyan.ietf@gmail.com

Adam Montville
Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
USA

Email: adam.w.montville@gmail.com

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301)975-4288
Email: sab3@nist.gov