Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 18, 2017

B. Munyan
A. Montville
Center for Internet Security
June 16, 2017

Definition of the ROLIE configuration checklist Extension draft-mandm-sacm-rolie-configuration-checklist-00

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 is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 18, 2017.

Table of Contents

1. Introduction

This document defines an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) protocol [I-D.ietf-mile-rolie] 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, security-minded configuration for each technology they operate. Such standard 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. New information-types

This document defines a new "information-type" value of "configuration-checklist".

3.1. The "configuration-checklist" information-type

The "configuration-checklist" information type represents a body of information describing a set of configuration recommendations. A configuration recommendation is, minimally, a single configuration item paired with a recommended value or range of values. 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. Usage of Configuration Checklist Information in the Atom Publishing Protocol

These requirements apply when a ROLIE repository contains any Collections, who's href points to an atom:feed who's atom:category element contains a scheme attribute of "urn:ietf:params:rolie:category:information-type" and a term attribute of the new "configuration-checklist" information-type.

```
<atom:category
  scheme="urn:ietf:params:rolie:category:information-type"
  term="configuration-checklist">...</atom:category>
```

5. Requirements for the 'atom:entry' Element

The following sections describe the various requirements for the "atom:entry" element, and it's child elements, when publishing configuration checklist information to a ROLIE repository.

5.1. The 'atom:content' Element

Information about the proposed serialization types for configuration checklists

- PDF

- Text

- Word

- Excel

- XML via DSC

- JSON?

5.2. The 'rolie:format' Element

A configuration checklist may be published by an organization using numerous formats, such as PDF, Word or Excel documents, and automation content using XML or JSON data models.

This document does not specify any additional requirements for use of the rolie:format element.

5.3. Configuration checklist metadata included in the 'rolie:property' Element

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.

- author (0..n)
  - An unbounded number of "rolie:property" elements with a "name" attribute of "author" may be included to indicate those individuals noted as the authors of the configuration checklist.
- 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"
- publication date
- overview

- Product category (0..n), 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

5.4. atom:link Registrations

TODO: Can there be multiple of these links? For example, I really want more than one target-platform and more than one profile.

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

6. 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.

New IANA table for "ROLIE Entry Format"

- 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

name: configuration-checklist

index: TBD

reference: TBD

7. Security Considerations

TBD

8. Privacy Considerations

TBD

9. References

9.1. Normative References

[I-D.ietf-mile-rolie]
Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange", draft-ietf-mile-rolie-07 (work in progress), May 2017.

9.2. 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>.

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