Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 14, 2021

S. Banghart
NIST
B. Munyan
A. Montville
Center for Internet Security
G. Alford
Red Hat, Inc.
July 13, 2020

Definition of the ROLIE configuration checklist Extension draft-mandm-sacm-rolie-configuration-checklist-02

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support security configuration checklist use cases. Additional categories, properties, and requirements based on content type enables a higher level of interoperability between ROLIE implementations, and richer metadata for ROLIE consumers. Additionally, this document discusses requirements and usage of other ROLIE elements in order to best syndicate security configuration checklists.

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 https://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 January 14, 2021.

Table of Contents

1. Introduction

Default configurations for endpoints (operating systems, applications, etc.) are normally geared towards ease-of-use or ease-of-deployment, not security. As such, 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. 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. 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

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The previous key words are used in this document to define the requirements for implementations of this specification. As a result, the key words in this document are not used for recommendations or requirements for the use of ROLIE.

As an extension of [RFC8322], this document refers to many terms defined in that document. In particular, the use of "Entry" and "Feed" are aligned with the definitions presented in section TODO of ROLIE.

Several places in this document refer to the "information-type" of a Resource (Entry or Feed). This refers to the "term" attribute of an "atom:category" element whose scheme is "urn:ietf:params:rolie:category:information-type". For an Entry, this value can be inherited from it’s containing Feed as per [RFC8322].

Other terminology used in this document is defined below:

Configuration Item Generally synonymous with endpoint attribute.

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

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: 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 registers a new information type for use in ROLIE repositories. 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

4. rolie:property Extensions

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.

This document registers several new rolie:property elements to express this metadata in a more efficient and automatable form.

- contributor (0..n)
  - name: urn:ietf:params:rolie:property:checklist:contributor

    * value: Indicates those individuals noted as recognized contributors to the configuration checklist and/or the recommendations contained within. The value MUST be either a plaintext name of a entity, or a link to an <author> element that describes an entity.

- checklist version
    * name: urn:ietf:params:rolie:property:checklist:version
    * value: Indicates the version/revision number of the configuration checklist. Implementations MAY choose to incorporate a semantic versioning scheme illustrating "major.minor.point" releases, such as "3.1.1".
- title
    * name: urn:ietf:params:rolie:property:checklist:title
    * value: Indicates the document title of the configuration checklist, such as "CIS Benchmark for Microsoft Windows Server 2019".
- overview
    * name: urn:ietf:params:rolie:property:checklist:overview
    * value: This property allows for a textual overview and/or introduction to the configuration checklist including, but not limited to, overview of the technology under assessment, limitations or caveats, or assumptions to be made when evaluating the checklist.
- product name (0..n)
    * name: urn:ietf:params:rolie:property:checklist:product-name
    * value: This property allows for further refinement and identification of the configuration checklist using the name of the product or products to which the checklist applies, such as Microsoft Windows Server 2019, Red Hat Enterprise Linux, IBM WebSphere Application Server, Google Chrome, etc.
- product category (0..n)
    * name: urn:ietf:params:rolie:property:checklist:product-category

* value: This property allows for further refinement and identification of the configuration checklist using the technology category. Examples of product category values may be (but aren't limited to):

  + 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. Handling Existing Checklist Formats

Today, checklists are distributed in a myriad of different formats, using a variety of organization schemes. This standard attempts to be as flexible as possible in its approach, in order to be usable by as many checklist distributors as possible.

Using the NIST National Checklist Program as a foundation, checklists consist of a primary set of content and a list of supporting content. These pieces of content come in a number of machine readable and

human readable formats, and it is out of scope of this standard to describe guidance for all them. Instead, a best effort should be made to use the available properties, elements, and attributes to describe the content. Moreover, the content is often a compressed file that consists of a package of other content. Likewise, describing this nested structure is out of scope for this standard. Each organization should use a description scheme that best matches their use and business cases, and this description scheme should be documented as thoroughly as possible for all users.

When existing identifiers, titles, authors, and dates are provided in machine-readable forms inside a ROLIE Entry, automated processes can find and acquire checklist content with more ease than the current state-of-the-art methodology. Fully solving the checklist automation problem will require a more significant effort touching on all parts of the checklist ecosystem.

6. atom:link Extensions

Name	Description
ancestor	Links to a configuration checklist superseded by that described in this entry
target-platform	Links to a software descriptor resource defining the software subject to this configuration checklist entry
supporting	Links to a supporting document for the main content. The "title" attribute SHOULD be used to provide a human readable title for this document. Where possible, the "type" attribute MAY be used to describe the type of the supporting document. If the type is a simple IANA Media Type, the media type text should be used, otherwise, a short human readable description should be used.

7. IANA Considerations

7.1. configuration-checklist information-type

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> .

The entry is as follows:

name: configuration-checklist

index: TBD

reference: This document, Section 3

7.2. checklist:constributor property

IANA has added an entry to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

The entry is as follows:

name: property:checklist:contributor

Extension IRI:
urn:ietf:params:rolie:property:checklist:contributor

Reference: This document, Section 4

Subregistry: None

8. Security Considerations

Use of this extension requires understanding and managing the security considerations of the core ROLIE specification. Beyond that, there must be considerations made for the common use cases and data types that would be shared with this extension in particular.

Checklist information, while typically shared publicly, can have potential security impact if compromised. In these cases, the utmost care should be taken to secure the REST endpoint. Ensure that only authenticated users are allowed request access to any part of the ROLIE repository. Authentication schemes such as OAUTH or basic HTTP Auth provides a significant barrier to compromise. When providing checklist information as a paid service, security is valuable as a means to protect valuable data from being stolen or taken for free. In these cases, the above strategies still apply, but providers may want to make the Feed visible to non-authenticated users, with meaningful error messages sent to users that have not yet paid for the service.

Typical RESTful security measures applied commonly on the web would be effective to secure this ROLIE extension. As a flexible and relatively simple RESTful service, ROLIE server implementations have great flexibility and freedom in securing their repository.

9. Privacy Considerations

This extension poses no additional privacy considerations above and beyond those stated in the core ROLIE specification.

10. References

10.1. 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.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

10.2. 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>.

Appendix A. Examples

This section provides some brief examples of a Checklist Information Type ROLIE Entry.

```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="https://www.w3.org/2005/Atom"
    xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0" xml:lang="en-US">
    <id>c8db0a93-4dcb-426e-997f-ba43c100b863</id>
    <title>NIST National Checklist for Red Hat Virtualization Host 4.x</title>
    <published>2020-06-29T18:13:51.0Z</published>
    <updated>2020-06-29T18:13:51.0Z</updated>
    <category scheme="urn:ietf:params:rolie:category:information-type" term="chec
klist"/>
    <summary>SCAP content for evaluation of Red Hat Virtualization Host 4.x syste
ms. The Red Hat content embeds multiple pre-established compliance profiles.</sum
mary>
    <rolie:format ns="scap13namespace"/>
    <content type="application/zip" src="https://nvd.nist.gov/ncp/checklist/908/d
ownload/5615"/>
    <link rel="supporting" title="OpenControl-formatted NIST 800-53 responses for
 Red Hat Virtualization Host 4.x" href="https://github.com/ComplianceAsCode/redha
t/tree/master/virtualization-host" type="Machine-Readable Format"/>
    <link rel="supporting" title="[DRAFT] DISA STIG for Red Hat Virtualization Ho
st (RHVH)" href="https://galaxy.ansible.com/RedHatOfficial/rhv4_rhvh_stig" type="
Ansible Playbook"/>
    <link rel="supporting" title="VPP - Protection Profile for Virtualization v.
1.0 for Red Hat Virtualization Hypervisor (RHVH)" href="https://galaxy.ansible.co
m/RedHatOfficial/rhv4_rhvh_vpp" type="Ansible Playbook"/>
    <rolie:property name="urn:ietf:params:rolie:property:content-id" value="908"/
>
    <rolie:property name="urn:ietf:params:rolie:property:checklist:checklist-vers
ion" value="content v0.1.48"/>
    <rolie:property name="urn:ietf:params:rolie:property:content-published-date"
value="2020-01-14T00:00:00+00:00"/>
    <rolie:property name="urn:ietf:params:rolie:property:content-updated-date" va
lue="2019-06-14T00:00:00+00:00"/>
    <rolie:property name="urn:ietf:params:rolie:property:checklist:product-catego
ry" value="Virtual Machine"/>
</entry>
```

Authors' Addresses

Stephen Banghart
NIST
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Email: stephen.banghart@nist.gov

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

Gabriel Alford
Red Hat, Inc.
100 East Davie Street
Raleigh, North Carolina 27601
USA

Email: galford@redhat.com