MILE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2020

S. Banghart
NIST

October 28, 2019

Definition of the ROLIE Vulnerability Extension
draft-ietf-mile-rolie-vuln-03

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Vulnerability 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. In particular, usage of the Common Vulnerability Enumeration (CVE) [cve] format is discussed.

Table of Contents

1. Introduction

As our software becomes more complex and interconnected, the number of software vulnerabilities exploitable by actors with mal-intent has skyrocketed. Huge amounts of resources have been poured into the preemptive discovery, description, and remediation of these vulnerabilities, but it is often a challenge to share and communicate the results of these efforts. While bad-actors have vast collaboration networks that enable widespread knowledge of any vulnerability, the defensive community at large has no sharing consortium as prevalent. If we are to keep up with the rising difficulty of defending our systems, we must increase our ability to quickly, efficiently, and automatically share information about vulnerabilities.

The Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] provides a means to share computer security information with an eye towards automation and efficiency. By utilizing ROLIE to share vulnerability data, we get one step closer to establishing automated communication between each party involved in fighting vulnerabilities. A security researcher can send a newly discovered vulnerability to a vulnerability repository, where it is automatically retrieved and consumed by enterprise systems. At this final stage, the enterprise can cross-reference against their enterprise wide software load to begin mitigating the issue.

This extension to ROLIE introduces new requirements and IANA registrations to allow ROLIE repositories to share vulnerability data in a standardized and compatible way.

This extension does not attempt to solve the vulnerability data format issue, as this work is being done across standards groups and industry consortiums. Instead, this extension serves to address the problem of sharing these data formats to downstream consumers in a automated and efficient fashion.

2. Terminology

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 [RFC8174].

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 there.

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].

This document uses the definition of "vulnerability" given by [RFC4949].

3. The "vulnerability" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid value for this attribute: "vulnerability", is described in this section, and registered in Section 6.1.1. When this value is used, the resource in question is considered to have an information-type of "vulnerability" as per [RFC8322] Section 7.1.2.

The "vulnerability" information-type represents any information describing or pertaining to a computer security vulnerability. This document uses the definition of vulnerability provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be of a vulnerability information type.

- Fundamental identifying information, such as a global ID or number, that identifies a given vulnerability.

- Descriptive information, including but not limited to:
  - Severity scoring - using some standardized scoring algorithm or otherwise,
  - Execution details - how the vulnerability is exploited
  - Impact - what the consequences are of this vulnerability
  - History and provenance data - when was the vulnerability discovered, when was it reported and to whom,
  - Plain text description of any of the above
- Metadata attached to a vulnerability, such as information about the entity that discovered or described the vulnerability.

Note again that this list is not exhaustive: any information that is in the abstract realm of a vulnerability should be classified under this information-type. The final decision as to the information type of an Entry is up to the provider and author of the Entry.

4. Common Vulnerability Enumeration (CVE) Format

4.1. Description

The Common Vulnerability Enumeration (CVE) provides a globally unique identifier for vulnerabilities. Each CVE provides a CVE-ID, by which a vulnerability can be referred to in any context, as well as descriptive information about that vulnerability.

For more information and in-depth specifications, please see [cve].

CVE provides a valuable set of information fields, but itself does not provide a standardized data format. This extension provides standardization around two common serializations of the CVE standard, both used by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD provides a repository of "CVE Entries" available in either serialization format. The first format is XML-based: the NIST NVD CVE Entry format [nvdcvexml], and the second is JSON-based: NIST NVD JSON CVE Entry Format [nvdcvejson]. These two representations of a CVE are equivalent, and can be losslessly converted.

This section defines usage guidance and additional requirements above and beyond those specified in [RFC8322] that apply when CVE data formats are in use.

4.2. Requirements

For an Entry to be considered a "CVE Entry", it MUST fulfill the following conditions:

- The information-type of the Entry is "vulnerability". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.

- The document linked to by the "ref" attribute of the "atom:content" element is a CVE Entry as defined by either [nvdcvexml] or [nvdcvejson]. Other well-defined CVE serializations would be valid but would not be subject to the following requirements, reducing their interoperability.

The XML and JSON NVD formats follow different requirements.

A "XML CVE Entry" MUST conform to the following requirements:

- The value of the "type" attribute of the "atom:content" element MUST be "application/xml".

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<name>" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

A "JSON CVE Entry" MUST conform to the following requirements:

- The value of the "type" attribute of the "atom:content" element MUST be "application/json".

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "cve:{cve_data_meta":{ID}}" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

5. Link relations for the 'vulnerability' information-type

The atom:link element contains a "rel" attribute that describes the semantic meaning of the given link.

If the category of an Entry is the vulnerability information type, then the following link relations MUST be respected, that is, not

removed, by the server. Implementations can provide extra functionality by understanding the semantic meaning of these relations.

Name	Description
severity	Links to a document describing or scoring the severity of this vulnerability.

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6. IANA Considerations

6.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type> .

6.1.1. vulnerability information-type

The entry is as follows:

name: vulnerability

index: TBD

reference: This document, Section 3

7. Security Considerations

All security considerations of the core ROLIE document apply to use of this extension.

The use of this particular extension implies the use of ROLIE in sharing vulnerability information. In automated use cases, downstream consumers may be dynamically acquiring and acting on vulnerabilities posted to a ROLIE repository. In this case, a compromised server could serve up false vulnerability information to trigger dangerous activity in automated consumers. Automatic remediation solutions that consume shared vulnerability information in high risk use cases should take care to verify data before taking action. If some global ID, such as a CVE-ID, is included, this verification should be trivial.

8. Normative References

[cve] "Common Vulnerability Enumeration", <https://cve.mitre.org/about/index.html>.

[cvexml] The MITRE Corporation, , <https://cve.mitre.org/schema/cve/cve_1.0.xsd>.

[nvdcvejson] National Institute of Standards and Technology, "NVD CVE Entry JSON Schema", <https://csrc.nist.gov/schema/nvd/feed/1.0/nvd_cve_feed_json_1.0.schema>.

[nvdcvexml] National Institute of Standards and Technology, "NVD CVE Entry XML Schema", <https://csrc.nist.gov/schema/nvd/nvdcve.xsdf>.

[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>.

[RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, DOI 10.17487/RFC4287, December 2005, <https://www.rfc-editor.org/info/rfc4287>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <https://www.rfc-editor.org/info/rfc5023>.

[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>.

Author's Address

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

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