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. The vulnerability information type is defined as a ROLIE extension. Additional supporting requirements are also defined that 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 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 September 27, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

Vulnerability information sharing is one of the main use cases listed in RFC8322. This document provides additional format specific requirements to support interoperability and rich metadata of vulnerability information shared using ROLIE.

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 [RFC2119].

Definitions for some of the common computer security-related terminology used in this document can be found in [RFC4949].

3. Information-type Extensions

Table of Contents

1. Introduction .................................................. 2
2. Terminology .................................................. 2
3. Information-type Extensions ................................. 2
   3.1. The "vulnerability" information type ..................... 3
4. Use of the rolie:format element ............................... 3
   4.1. CVE Format ............................................. 3
   4.2. VDO Format ............................................. 3
5. rolie:property Extensions ...................................... 3
6. Use of the atom:link element ................................ 3
   6.1. Link relations for the ‘vulnerability’
        information-type ....................................... 4
7. IANA Considerations ........................................... 4
   7.1. information-type registrations ............................ 4
      7.1.1. vulnerability information-type ....................... 4
   7.2. rolie:property name registrations .......................... 4
      7.2.1. property:vulnerability:id ............................ 4
8. Security Considerations ....................................... 5
9. Normative References ......................................... 5
Author’s Address ................................................. 5
3.1. The "vulnerability" information type

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.

o TODO

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.

4. Use of the rolie:format element

4.1. CVE Format

Todo

4.2. VDO Format

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 the information they are looking for.

5.1. urn:ietf:params:rolie:property:vuln:ID

Provides an XML element that can be populated with an identifier from the vulnerability document linked to by an atom:content element. This value SHOULD be a uniquely identifying value for the document linked to in this entry’s atom:content element.

6. Use of the atom:link element

These sections define requirements for atom:link elements in Entries. Note that the requirements are determined by the information type that appears in either the Entry or in the parent Feed.
6.1. Link relations for the 'vulnerability' information-type

If the category of an Entry is the vulnerability information type, then the following requirements MUST be followed for support of atom:link elements.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>todo</td>
<td>todo</td>
<td>todo</td>
</tr>
</tbody>
</table>

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

7. IANA Considerations

7.1. 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>.

7.1.1. vulnerability information-type

The entry is as follows:

name: vulnerability

index: TBD

reference: This document, Section 3.1

7.2. rolie:property name registrations

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

7.2.1. property:vulnerability:id

The entry is as follows:

name: property:vulnerability:id


Reference: This document, section 6.3.1
8. Security Considerations

This document implies the use of ROLIE in high-security use cases, as such, added care should be taken to fortify and secure ROLIE repositories and clients using this extension. The guidance in the ROLIE core specification is strongly recommended, and implementers should consider adding additional security measures as they see fit.

When providing a private workspace for closed sharing, it is recommended that the ROLIE repository checks user authorization when the user sends a GET request to the service document. If the user is not authorized to send any requests to a given workspace or collection, that workspace or collection should be truncated from the service document in the response. In this way the existence of unauthorized content remains unknown to potential attackers, hopefully reducing attack surface.

9. Normative References


Author’s Address