Internet Engineering Task Force (IETF)
Request for Comments: 7495
Category: Standards Track
ISSN: 2070-1721

A. Montville
CIS
D. Black
EMC

March 2015

Enumeration Reference Format for the Incident Object Description Exchange Format (IODEF)

Abstract

The Incident Object Description Exchange Format (IODEF) is an XML data representation framework for sharing information about computer security incidents. In IODEF, the Reference class provides references to externally specified information such as a vulnerability, Intrusion Detection System (IDS) alert, malware sample, advisory, or attack technique. In practice, these references are based on external enumeration specifications that define both the enumeration format and the specific enumeration values, but the IODEF Reference class (as specified in IODEF v1 in RFC 5070) does not indicate how to include both of these important pieces of information.

This document establishes a stand-alone data format to include both the external specification and specific enumeration identification value, and establishes an IANA registry to manage external enumeration specifications. While this document does not update IODEF v1, this enumeration reference format is used in IODEF v2 and is applicable to other formats that support this class of enumeration references.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7495.

Table of Contents

1. Introduction

There is an identified need to specify a format to include relevant enumeration values from other data representation formats in an IODEF document. It is anticipated that this requirement will exist in other standardization efforts within several IETF Working Groups, but the scope of this document pertains solely to IODEF. This format is used in IODEF v2 [IODEFv2], which will replace the original IODEF v1 [IODEF] specification; this document does not specify use of this format in IODEF v1 [IODEF].

1.1. 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 RFC 2119 [RFC2119].

2. Referencing External Enumerations

The need is to place enumeration identifiers and their enumeration format references in IODEF's Reference class. There are several ways to accomplish this goal, but the most appropriate at this point is to require a specific structure for the ReferenceName string of the IODEF Reference class, and use an IANA registry to manage references to specific enumeration reference formats.

Per IODEF [IODEF], the ReferenceName is of type ML_STRING. This becomes problematic when specific references, especially enumeration formats such as Common Vulnerability Enumeration [CVE], Common Configuration Enumeration [CCE], Common Platform Enumeration [CPE], and so on, are referenced -- how is an implementer to know which type of reference this is, and thus how to parse it? One solution, presented here, is to require that ReferenceName follow a particular format.

Inclusion of such enumeration values, especially those related to security automation, is important to incident communication and investigation. Typically, an enumeration identifier is simply an identifier with a specific format as defined by an external party. Further, that enumeration identifier is itself a reference to specific information associated with the identifier. Thus, the ReferenceName is an identifier that is formatted in a specific manner and that identifies some set of associated information.

For example, a vulnerability identifier following the CVE [CVE] formatting specification may be CVE-2014-0001. That identifier is formatted in a specific manner and relates to information about a specific vulnerability. Communicating the format for the identifier is the subject of this document.

2.1. Reference Name Format

The ReferenceName class provides the XML representation for identifying an enumeration and specifying a value from it. A given enumeration is uniquely identified by the specIndex attribute. Each specIndex value corresponds to an entry in the "Enumeration Reference Type Identifiers" IANA registry (see Section 4). The child ID element represents a particular value from the corresponding enumeration identified by the specIndex attribute. The format of the ID element is described in the IANA registry entry of the enumeration.

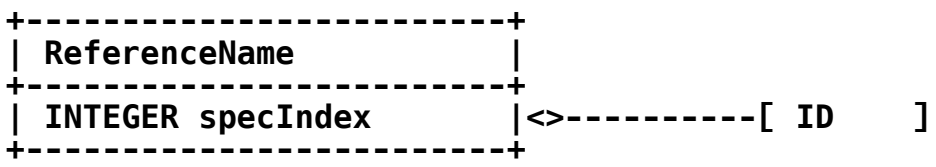

Figure 1: The ReferenceName Class

The aggregate class that constitutes ReferenceName is:

ID
: One. The identifier assigned to represent the particular enumeration object being referenced.

The ReferenceName class has one attribute.

specIndex
: Required. INTEGER. Enumeration identifier. This value corresponds to an entry in the "Enumeration Reference Type Identifiers" IANA registry with an identical SpecIndex value.

An example of such a reference is as follows:

```
<iodef:Reference>
   <enum:ReferenceName specIndex="1">
      <enum:ID>CXI-1234-XYZ</enum:ID>
   </enum:ReferenceName>
   <iodef:URL>http://cxi.example.com</iodef:URL>
   <iodef:Description>Foo</iodef:Description>
</iodef:Reference>
```

Information in the IANA table (see Section 4) would include:

```
Full Name: Concept X Identifier
SpecIndex: 1
Version: any
Specification URI: http://cxi.example.com/spec_url
```

2.2. Reference Method Applicability

While the scope of this document pertains to IODEF, any standard needing to reference an enumeration identified by a specially formatted string can use this method of providing structure after the standard has been published. In effect, this method provides a standardized interface for enumeration formats, thus allowing a loose coupling between a given standard and the enumeration identifiers it needs to reference now and in the future.

3. Security Considerations

Ensuring a proper mapping of enumeration reference ID elements to the correct SpecIndex is important. Potential consequences of not mapping correctly include inaccurate information in references and similar distribution of misinformation.

Use of enumeration reference IDs from trusted sources is preferred to mitigate the risk of receiving and/or providing misinformation. Trust decisions with respect to enumeration reference providers are beyond the scope of this document. However, receiving an IODEF [IODEF] document containing an unknown ReferenceName (i.e., the SpecIndex does not exist in the IANA table) may indicate a misled or malicious source.

This document establishes a container for publicly available enumeration values to be included in an IODEF [IODEF] document, and it is important to note the distinction between the enumeration value's format and the information conveyed by the value itself. While the enumeration value may hold information deemed to be private by relying parties, the enumeration format is likely not subject to privacy concerns.

However, if the Reference class includes an enumeration value in combination with other data in an IODEF [IODEF] document, the resulting combination could expose information. An example might include attack vectors or system descriptions used in a privacy-related incident. As such, the reader is referred to the IODEF [IODEF] Security Considerations section, which explicitly covers protecting IODEF [IODEF] documents in transit and at rest, ensuring

proper recipient authentication, data confidence levels, underlying transport security characteristics, and proper use of IODEF's restriction attribute.

4. IANA Considerations

This document specifies an enumeration reference identifier format. All fields, including abbreviation, are mandatory.

Per this document, IANA has created and maintains the following registry:

Name of the Registry: "Security External Enumeration Registry"

Location of Registry: http://www.iana.org/assignments/sec-ext-enum

Fields to record in the registry:

Full Name: The full name of the enumeration (i.e., the referenced specification) as a string from the printable ASCII character set [RFC20] with individual embedded spaces allowed. The ABNF [RFC5234] syntax for this field is:

```
FULL-NAME = 1*VCHAR *(SP 1*VCHAR)
```

Abbreviation: An abbreviation may be an acronym -- it consists of uppercase characters (at least two). Uppercase is used to avoid mismatches due to case differences. It is specified by this ABNF [RFC5234] syntax:

```
ABBREVIATION = 2*UC-ALPHA      ; At least two
UC-ALPHA = %x41-5A             ; A-Z
```

Multiple registrations MAY use the same Abbreviation but MUST have different Versions.

SpecIndex: This is an IANA-assigned positive integer that identifies the registration. The first entry added to this registry uses the value 1, and this value is incremented for each subsequent entry added to the registry.

Version: The version of the enumeration (i.e., the referenced specification) as a free-form string from the printable ASCII character set [RFC20] excepting white space, i.e., from VCHAR as defined in [RFC5234]. Some of the characters allowed in the version string are escaped when that string is used in XML

documents (e.g., '<' is represented as <); the registered version string contains the unescaped ASCII character in all such cases.

Specification URI/Reference: A list of one or more URIs [RFC3986] from which the registered specification can be obtained. The registered specification MUST be readily and publicly available from that URI. The URI SHOULD be a stable reference to a specific version of the specification. URIs that designate the latest version of a specification (which changes when a new version appears) SHOULD NOT be used.

Initial registry contents:

Full Name: Common Vulnerabilities and Exposures

Abbreviation: CVE

SpecIndex: 1

Version: 1.0

Specification URI/Reference: https://nvd.nist.gov/download.cfm#CVE_FEED

Allocation Policy: Specification Required [RFC5226] (which implies Expert Review [RFC5226]).

The Designated Expert is expected to consult with the MILE (Managed Incident Lightweight Exchange) working group or its successor if any such WG exists (e.g., via email to the working group's mailing list). The Designated Expert is expected to review the request and validate the appropriateness of the enumeration for the attribute. This review includes review of the specification associated with the request.

The Designated Expert is expected to ensure that the Full Name, Abbreviation, and Version are appropriate and that the information at the Specification URI is sufficient to unambiguously parse identifiers based on that specification. Additionally, the Designated Expert should prefer short Abbreviations over long ones.

This document uses URNs to describe XML namespaces and XML schemas conforming to a registry mechanism described in [RFC3688].

Registration for the IODEF enumeration reference format namespace:

URI: urn:ietf:params:xml:ns:iodef-enum-1.0

Registrant Contact: See the "Authors' Addresses" section of this document.

XML: None.

Registration for the IODEF enumeration reference format XML schema:

URI: urn:ietf:params:xml:schema:iodef-enum-1.0

Registrant Contact: See the "Authors' Addresses" section of this document.

XML: See Section 5, "The ReferenceName Schema", of this document.

5. The ReferenceName Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified"
      elementFormDefault="qualified"
      targetNamespace="urn:ietf:params:xml:ns:iodef-enum-1.0"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:enum="urn:ietf:params:xml:ns:iodef-enum-1.0">

 <!--
 ============================================================
 ===  ReferenceName                                       ===
 ============================================================
  -->
 <xs:element name="ReferenceName">
   <xs:complexType>
     <xs:sequence>
       <xs:element name="ID" type="xs:NCName"/>
     </xs:sequence>
     <xs:attribute name="specIndex"
                   type="xs:integer" use="required"/>
   </xs:complexType>
 </xs:element>
</xs:schema>
```

6. References

6.1. Normative References

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

[IODEF] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007, <http://www.rfc-editor.org/info/rfc5070>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004, <http://www.rfc-editor.org/info/rfc3688>.

6.2. Informative References

[RFC20] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, October 1969, <http://www.rfc-editor.org/info/rfc20>.

[IODEFv2] Danyliw, R. and P. Stoecker, "The Incident Object Description Exchange Format v2", Work in Progress, draft-ietf-mile-rfc5070-bis-11, March 2015.

[CCE] The MITRE Corporation, "Common Configuration Enumeration (CCE): Unique Identifiers for Common System Configuration Issues", website in "Archive" status, <http://cce.mitre.org>.

[CPE] The MITRE Corporation, "CPE - Common Platform Enumeration", website in "Archive" status, <http://cpe.mitre.org>.

[CVE] The MITRE Corporation, "CVE - Common Vulnerabilities and Exposures", <http://cve.mitre.org>.

Acknowledgements

The authors would like to thank Eric Burger for the recommendation to rely on XML, Roman D. Danyliw for his schema contribution and insight, and Tim Bray, Panos Kampanakis, Barry Leiba, Ted Lemon, Alexey Melnikov, Kathleen Moriarty, Takeshi Takahashi, Henry S. Thompson, and David Waltermire for their contributions and reviews.

Authors' Addresses

Adam W. Montville

EMail: adam.w.montville@gmail.com

David Black
EMC Corporation

EMail: david.black@emc.com