

INTERNET-DRAFT
Intended Status: Standards Track
Updates: 5070 (if approved)
Expires: December 22, 2014

Adam W. Montville
(Tripwire)
David Black
(EMC)

June 20, 2014

IODEF Enumeration Reference Format
draft-ietf-mile-enum-reference-format-06

Abstract

The Incident Object Description Exchange Format (IODEF) provides a Reference class used to reference external entities (such as enumeration identifiers). However, the method of external entity identification has been left unstructured. This document describes a method to provide structure for referencing external entities for the IODEF Reference class and thus updates IODEF's ReferenceName (RFC5070).

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2014 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 (<http://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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1	Introduction	3
1.1	Terminology	3
2.	Referencing External Enumerations	3
3	Security Considerations	5
4	IANA Considerations	5
5	IODEF XML Schema Changes	6
6	References	8
6.1	Normative References	8
6.2	Informative References	8
	Authors' Addresses	8

1 Introduction

There is an identified need to specify a format to include relevant enumeration values 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 [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 references in IODEF [IODEF]'s Reference class. There are several ways to accomplish this goal, but the most appropriate at this point is to require a specific format for the ReferenceName string of the IODEF [IODEF] Reference class, and use an IANA registry to manage the resulting reference formats.

```
+-----+
| Reference |
+-----+
|           |<>-----[ ReferenceName ]
|           |<>--{0..*}--[ URL           ]
|           |<>--{0..*}--[ Description   ]
+-----+
```

FIGURE 1: IODEF [IODEF] Reference Class

Per IODEF [IODEF] the ReferenceName is of type ML_STRING. This becomes problematic when specific references, especially enumerations such as CVE [CVE], CCE [CCE], CPE [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 enumerations, 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.

2.1 Reference Name Format

The Reference Name Format uses XML to provide the structure for enumeration identification, and requires that a specific Index be associated with the ID. An implementer can look up the ID type (as referenced by the Index) in the IANA table (see Section 4) to understand how the ID is structured. The Index field in the XML unambiguously indicates which IANA registry entry is to be used to correctly reference the enumeration specification, which avoids interpretation of version strings that may have specification-specific formats.

```
<Reference>
  <ReferenceName>
    <Index>1</Index>
    <ID>CXI-1234-XYZ</ID>
  </ReferenceName>
  <URL>http://cxi.example.com</URL>
  <Description>Foo</Description>
</Reference>
```

LISTING 1: Example Use of IODEF Enumeration Reference Format

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

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

2.3 Reference Method Applicability

While the scope of this document pertains to IODEF [IODEF], it should be readily apparent that 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 enumerations, 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

Producers of IODEF [IODEF] content SHOULD be careful to ensure a proper mapping of enumeration reference ID elements to the correct Index. Potential consequences of not mapping correctly include inaccurate information references and similar distribution of misinformation.

Use of enumeration reference IDs from trusted sources SHOULD be preferred by implementers to mitigate the risk of receiving and/or providing misinformation. Trust decisions with respect to enumeration reference providers is beyond the scope of this document.

In some cases it might be possible for a third-party to host content associated with an enumeration reference ID. In such a circumstance, trust SHOULD extend from the origin of the enumeration reference ID to the third-party, effectively making the third-party a trusted third-party in the context of providing a particular set of enumeration reference IDs.

4 IANA Considerations

This document specifies an identifier format for the IODEF [IODEF] ReferenceName string of the Reference class.

This memo creates the following registry for IANA to manage:

Name of the Registry: "Enumeration Reference Type Identifiers"

Fields to record in the registry:

Full Name: The full name of the enumeration as a string from the printable ASCII character set.

Abbreviation: An abbreviation may be an acronym - it consists of upper-case characters (at least two, upper-case is used to avoid mismatches due to case differences), as 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.

Index: 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 as a free-form string from the printable ASCII character set excepting white space.

Specification URI: 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: None.

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. If a specification is associated with the request, it MUST be reviewed by the Designated Expert.

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.

5 IODEF XML Schema Changes

The changes to the IODEF [IODEF] schema are detailed below. Note that in addition to the element changes described below, certain attributes of the `xs:schema` element in the schema document should be updated, as well as certain information in the document class.

The `xs:schema` attributes are updated as follows:

```
targetNamespace="urn:ietf:params:xml:ns:iodef-1.01"
```

```
xmlns="urn:ietf:params:xml:ns:iodef-1.01"
```

```
xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.01"
```

The IODEF-Document element description is updated to have a fixed version of "1.01" instead of "1.00", such that:

```
<xs:element name="IODEF-Document">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Incident" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:string" fixed="1.00"/>
    <xs:attribute name="lang" type="xs:language" use="required"/>
    <xs:attribute name="formatid" type="xs:string"/>
  </xs:complexType>
</xs:element>
```

Is changed to:

```
<xs:element name="IODEF-Document">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Incident" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:string" fixed="1.01"/>
    <xs:attribute name="lang" type="xs:language" use="required"/>
    <xs:attribute name="formatid" type="xs:string"/>
  </xs:complexType>
</xs:element>
```

The ReferenceName element is updated by replacing the following line in the 1.00 schema:

```
<xs:element name="ReferenceName" type="iodef:MLStringType"/>
```

With:

```
<xs:element name="ReferenceName">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Index" type="xs:integer"/>
      <xs:element name="ID" type="xs:NCName"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

LISTING 2: IODEF Enumeration Reference Format Schema Changes

This change to the IODEF [IODEF] schema may cause interoperability issues depending on tool implementation. If strict schema validation is used by a 1.00 tool when parsing an incoming IODEF [IODEF] 1.01

document, the elements under ReferenceName may not be understood and could cause errors. If strict schema validation is not used when parsing an incoming IODEF [IODEF] 1.01 document with a 1.00 tool, the elements under ReferenceName should simply be present in the object model, but this may lead to unpredictable results.

Implementers are encouraged to update their code to handle the IODEF [IODEF] 1.00 schema and the 1.01 schemas explicitly to avoid any unhandled exceptions that may occur when a 1.00 implementation attempts to parse a 1.01 document.

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.
- [IODEF] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
- [RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

6.2 Informative References

- [CCE] <http://cce.mitre.org>
- [CPE] <http://cpe.mitre.org>
- [CVE] <http://cve.mitre.org>

Authors' Addresses

Adam W. Montville

Email: adam@stoicsecurity.com

David Black

EMC Corporation

Email: david.black@emc.com