Security Automation and Continuous Monitoring M. Cokus
Internet-Draft D. Haynes
Intended status: Informational D. Rothenberg
Expires: March 11, 2017 The MITRE Corporation
J. Gonzalez
Department of Homeland Security
September 7, 2016

OVAL(R) Directives Model
draft-rothenberg-sacm-oval-directives-model-01

Abstract

This document specifies Version 5.11.1 of the OVAL Directives Model which defines the constructs used to tailor the level of detail contained within a set of OVAL Results.

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 http://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 March 11, 2017.

Table of Contents

1. Introduction

The Open Vulnerability and Assessment Language (OVAL) [OVAL-WEBSITE] is an international, information security community effort to standardize how to assess and report upon the machine state of systems. For over ten years, OVAL has been developed in

collaboration with any and all interested parties to promote open and publicly available security content and to standardize the representation of this information across the entire spectrum of security tools and services.

OVAL provides an established framework for making assertions about a system's state by standardizing the three main steps of the assessment process: representing the current machine state; analyzing the system for the presence of the specified machine state; and representing the results of the assessment which facilitates collaboration and information sharing among the information security community and interoperability among tools.

This draft is the part of the OVAL contribution to the IETF SACM WG that standardizes the representation of the results of an assessment. It is intended to serve as a starting point for the endpoint posture assessment data modeling needs of SACM specifically a capability to specify the level of detail in Evaluation Results.

1.1. Requirements Language

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. OVAL Directives Model

The OVAL Directives Model is used to control what result information is included in the OVAL Results as well as specify its level of detail.

Property	Type	Count	Description
generator	oval:GeneratorType	1	Information regarding the generation of the OVAL Directives content. The timestamp property of the generator MUST represent the time at which the oval_directives was created.
directives	oval-res:DefaultDirectivesType	1	Describes the default set of directives that specify the results that have been included in the OVAL Results.
class_directives	oval-res:ClassDirectivesType	0..5	Describes the set of directives that specify the class-specific results that

				have been included in the OVAL Results.
signature	ext:Signature	0..1		Mechanism to ensure the integrity and authenticity of the OVAL Directives content.

Table 1: oval_directives Construct

3. OVAL Directives Model Schema

The XML Schema that implements this OVAL Directives Model can be found below.

```
        <?xml version="1.0" encoding="utf-8"?>
<xsd:schema
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
     xmlns:oval-res=
     "http://oval.mitre.org/XMLSchema/oval-results-5"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:sch="http://purl.oclc.org/dsdl/schematron"
     xmlns:oval-dir=
     "http://oval.mitre.org/XMLSchema/oval-directives-5"
     targetNamespace=
     "http://oval.mitre.org/XMLSchema/oval-directives-5"
     elementFormDefault="qualified" version="5.11">
     <xsd:import namespace=
          "http://oval.mitre.org/XMLSchema/oval-common-5"
          schemaLocation="oval-common-schema.xsd"/>
     <xsd:import namespace=
          "http://oval.mitre.org/XMLSchema/oval-results-5"
          schemaLocation="oval-results-schema.xsd"/>
     <xsd:import
          namespace="http://www.w3.org/2000/09/xmldsig#"
          schemaLocation="xmldsig-core-schema.xsd"/>
     <xsd:annotation>
          <xsd:documentation>The following is a
               description of the elements, types,
               and attributes that compose the
```



```
               core schema for encoding Open
               Vulnerability and Assessment
               Language (OVAL) Directives. Each of
               the elements, types, and attributes
               that make up the Core Directives
               Schema are described in detail and
               should provide the information
               necessary to understand what each
               object represents. This document is
               intended for developers and assumes
               some familiarity with XML. A high
               level description of the
               interaction between these objects
               is not outlined
               here.</xsd:documentation>
          <xsd:appinfo>
               <schema>Core Directives</schema>
               <version>5.11.1</version>
               <date>4/22/2015 09:00:00 AM</date>
               <terms_of_use>Copyright (C) 2010 United States
                 Government. All Rights Reserved.</terms_of_use>
               <sch:ns prefix="oval-dir" uri=
                "http://oval.mitre.org/XMLSchema/
                oval-directives-5"
               />
          </xsd:appinfo>
     </xsd:annotation>
     <!-- ================================================= -->
     <!-- ================================================= -->
     <!-- ================================================= -->
```

```
        <xsd:element name="oval_directives">
             <xsd:annotation>
                  <xsd:documentation>The
                       oval_directives element is the
                       root of an OVAL Directive
                       Document. Its purpose is to
                       bind together the generator
                       and the set of directives
                       contained in the document. The
                       generator section must be
                       present and provides
                       information about when the
                       directives document was
                       compiled and under what
                       version. The optional
                       Signature element allows an
                       XML Signature as defined by
                       the W3C to be attached to the
```



```
                       document. This allows
                       authentication and data
                       integrity to be provided to
                       the user. Enveloped signatures
                       are supported. More
                       information about the official
                       W3C Recommendation regarding
                       XML digital signatures can be
                       found at
                       http://www.w3.org/TR/xmldsig-core/.
                  </xsd:documentation>
             </xsd:annotation>
             <xsd:complexType>
                  <xsd:sequence>
                       <xsd:element name="generator"
                            type="oval:GeneratorType">
                            <xsd:annotation>
                            <xsd:documentation>The
                            required generator
                            section provides
                            information about when
                            the directives document
                            was compiled and under
                            what
                            version.</xsd:documentation>
                            </xsd:annotation>
                       </xsd:element>
                       <xsd:element name="directives"
                            type="oval-res:DefaultDirectivesType">
                            <xsd:annotation>
                            <xsd:documentation>The
                            required directives
                            section presents flags
                            describing what
                            information must be been
                            included in an oval
                            results document. This
                            element represents the
                            default set of
                            directives. These
                            directives apply to all
                            classes of definitions
                            for which there is not a
                            class specific set of
                            directives.</xsd:documentation>
                            </xsd:annotation>
                       </xsd:element>
                       <xsd:element
```



```
                            name="class_directives"
                            type="oval-res:ClassDirectivesType"
                            minOccurs="0"
                            maxOccurs="5">
```

```
                    <xsd:annotation>
                    <xsd:documentation>The
                    optional class_directives
                    section presents flags
                    describing what
                    information has been
                    included in the results
                    document for a specific
                    OVAL Definition class.
                    The directives for a
                    particlar class override
                    the default
                    directives.</xsd:documentation>
                    </xsd:annotation>
               </xsd:element>
               <xsd:element
                    ref="ds:Signature"
                    minOccurs="0"
                    maxOccurs="1">
                    <xsd:annotation>
                    <xsd:documentation>The
                    optional Signature
                    element allows an XML
                    Signature as defined by
                    the W3C to be attached to
                    the document. This allows
                    authentication and data
                    integrity to be provided
                    to the user. Enveloped
                    signatures are supported.
                    More information about
                    the official W3C
                    Recommendation regarding
                    XML digital signatures
                    can be found at
                    http://www.w3.org/TR/xmldsig-core/.
                    </xsd:documentation>
                    </xsd:annotation>
               </xsd:element>
          </xsd:sequence>
     </xsd:complexType>
     <xsd:unique name="UniqueDirectiveClass">
          <xsd:annotation>
               <xsd:documentation>The class
```



```
                    attribute on
                    class_directives must be
                    unique.</xsd:documentation>
               </xsd:annotation>
               <xsd:selector
                    xpath="oval-dir:class_directives"/>
               <xsd:field xpath="@class"/>
          </xsd:unique>
     </xsd:element>

     <!-- ================================================= -->
     <!-- ==================  GENERATOR  ================== -->
     <!-- ================================================= -->
     <!--
          The GeneratorType is defined by the
          oval-common-schema. Please refer to that
          documentation for a description of the complex type.
     -->
     <!-- ================================================= -->
     <!-- =================  DIRECTIVES  ================== -->
     <!-- ================================================= -->
     <!--
          The DefaultDirectivesType is defined by the
          oval-results-schema.  Please refer to that
          documentation for a description of the complex type.
     -->
     <!-- ================================================= -->
     <!-- ================  DIRECTIVES  ================== -->
     <!-- ================================================= -->
     <!--
          The ClassDirectivesType is defined by the
          oval-results-schema.  Please refer to that
          documentation for a description of the complex type.
     -->
```

```
</xsd:schema>
```

4. Intellectual Property Considerations

DHS, on behalf of the United States, owns the registered OVAL trademarks, identifying the OVAL STANDARDS SUITE and any component part, as that suite has been provided to the IETF Trust. A "(R)" will be used in conjunction with the first use of any OVAL trademark in any document or publication in recognition of DHS's trademark ownership.

5. Acknowledgements

The authors wish to thank DHS for sponsoring the OVAL effort over the years which has made this work possible. The authors also wish to thank the original authors of this document Jonathan Baker, Matthew Hansbury, and Daniel Haynes of the MITRE Corporation as well as the OVAL Community for its assistance in contributing and reviewing the original document. The authors would also like to acknowledge Dave Waltermire of NIST for his contribution to the development of the original document.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

While OVAL is just a set of data models and does not directly introduce security concerns, it does provide a mechanism by which to represent endpoint posture assessment information. This information could be extremely valuable to an attacker allowing them to learn about very sensitive information including, but, not limited to: security policies, systems on the network, criticality of systems, software and hardware inventory, patch levels, user accounts and much more. To address this concern, all endpoint posture assessment information should be protected while in transit and at rest. Furthermore, it should only be shared with parties that are authorized to receive it.

Another possible security concern is due to the fact that content expressed as OVAL has the ability to impact how a security tool operates. For example, content may instruct a tool to collect certain information off a system or may be used to drive follow-up actions like remediation. As a result, it is important for security tools to ensure that they are obtaining OVAL content from a trusted source, that it has not been modified in transit, and that proper validation is performed in order to ensure it does not contain malicious data.

8. Change Log

8.1. -00 to -01

There are no textual changes associated with this revision. This revision simply reflects a resubmission of the document so that it remains in active status.

9. References

9.1. Normative References

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

9.2. Informative References

[OVAL-WEBSITE]
The MITRE Corporation, "The Open Vulnerability and Assessment Language", 2015, <http://ovalproject.github.io/>.

Authors' Addresses

Michael Cokus
The MITRE Corporation
903 Enterprise Parkway, Suite 200
Hampton, VA 23666
USA

Email: msc@mitre.org

Daniel Haynes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: dhaynes@mitre.org

David Rothenberg
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: drothenberg@mitre.org

Juan Gonzalez
Department of Homeland Security
245 Murray Lane
Washington, DC 20548
USA

Email: juan.gonzalez@dhs.gov