- Open Vulnerability and Assessment Language - Element Dictionary

- Schema: Linux Definition
- Version: 5.0 release candidate 3
- Release Date: 26 May 2006

The following is a description of the elements, types, and attributes that compose the Linux specific tests found in Open Vulnerability and Assessment Language (OVAL). Each test is an extension of the standard test element defined in the Core Definition Schema. Through extension, each test inherits a set of elements and attributes that are shared amongst all OVAL tests. Each test is described in detail and should provide the information necessary to understand what each element and attribute represents. This document is intended for developers and assumes some familiarity with XML. A high level description of the interaction between the different tests and their relationship to the Core Definition Schema is not outlined here.

The OVAL Schema is maintained by The Mitre Corporation and developed by the public OVAL Community. For more information, including how to get involved in the project and how to submit change requests, please visit the OVAL website at http://oval.mitre.org.

< dpkginfo_test >

The dpkginfo test is used to check information for a given DPKG package. It extends the standard TestType as defined in the oval-definitions-schema and one should refer to the TestType description for more information. The required object element references a dpkginfo_object and the optional state element specifies the data to check. The evaluation of the test is guided by the check attribute that is inherited from the TestType.

Child Elements	Type	MinOccurs	MaxOccurs
object	oval-def:ObjectRefType	1	1
state	oval-def:StateRefType	0	1

< dpkginfo_object >

The dpkginfo_object element is used by a dpkginfo test to define the object to be evaluated. Each object extends the standard ObjectType as definied in the oval-definitions-schema and one should refer to the ObjectType description for more information. The common set element allows complex objects to be created using filters and set logic. Again, please refer to the description of the set element in the oval-definitions-schema.

A dpkginfo object consists of a single name entity that identifies the package being checked.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-def:EntityObjectStringType	1	1

< dpkginfo_state >

The dpkginfo_state element defines the different information that can be used to evaluate the specified DPKG package. This includes the architecture, epoch number, release, and version numbers. Please refer to the individual elements in the schema for more details about what each represents.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-def:EntityStateStringType	0	1
arch	oval-def:EntityStateStringType	0	1
epoch	oval-def:EntityStateStringType	0	1
release	oval-def:EntityStateStringType	0	1
version	oval-def:EntityStateStringType	0	1
evr	oval-def:EntityStateStringType	0	1

< inetlisteningservers_test >

The inet listening servers test is used to check what applications are listening on the network. It is generally using the parsed output of running the command netstat -tuwlnpe with root privilege. It extends the standard TestType as defined in the oval-definitions-schema and one should refer to the TestType description for more information. The required object element references an inetlisteningservers_object and the optional state element specifies the data to check. The evaluation of the test is guided by the check attribute that is inherited from the TestType.

Child Elements	Type	MinOccurs	MaxOccurs
object	oval-def:ObjectRefType	1	1
state	oval-def:StateRefType	0	1

< inetlisteningservers_object >

The inetlisteningservers_object element is used by an inet listening servers test to define the specific protocol-address-port to be evaluated. Each object extends the standard ObjectType as definied in the oval-definitions-schema and one should refer to the ObjectType description for more information. The common set element allows complex objects to be created using filters and set logic. Again, please refer to the description of the set element in the oval-definitions-schema.

An inet listening servers object consists of three entities. The first identifies a specific ip address. The second entity represents a certain port number. While the third identifies the protocol.

Child Elements	Type	MinOccurs	MaxOccurs
protocol	oval-def:EntityObjectStringType	1	1
local_address	oval-def:EntityObjectStringType	1	1
local_port	oval-def:EntityObjectStringType	1	1

< inetlisteningservers_state >

The inetlisteningservers_state element defines the different information that can be used to evaluate the specified inet listening server. This includes the local address, foreign address, port information, and process id. Please refer to the individual elements in the schema for more details about what each represents.

Child Elements	Type	MinOccurs	MaxOccurs
protocol	oval-def:EntityStateStringType	0	1
local_address	oval-def:EntityStateStringType	0	1
local_port	oval-def:EntityStateStringType	0	1
local_full_address	oval-def:EntityStateStringType	0	1
program_name	oval-def:EntityStateStringType	0	1
foreign_address	oval-def:EntityStateStringType	0	1
foreign_port	oval-def:EntityStateStringType	0	1
foreign_full_address	oval-def:EntityStateStringType	0	1
pid	oval-def:EntityStateIntType	0	1
user_id	oval-def:EntityStateStringType	0	1

< rpminfo_test >

The rpm info test is used to check the RPM header information for a given RPM package. It extends the standard TestType as defined in the oval-definitions-schema and one should refer to the TestType description for more information. The required object element references a rpminfo_object and the optional state element specifies the data to check. The evaluation of the test is guided by the check attribute that is inherited from the TestType.

Child Elements	Type	MinOccurs	MaxOccurs

object	oval-def:ObjectRefType	1	1
state	oval-def:StateRefType	0	1

< rpminfo_object >

The rpminfo_object element is used by a rpm info test to define the object to be evaluated. Each object extends the standard ObjectType as definied in the oval-definitions-schema and one should refer to the ObjectType description for more information. The common set element allows complex objects to be created using filters and set logic. Again, please refer to the description of the set element in the oval-definitions-schema.

A rpm info object consists of a single name entity that identifies the package being checked.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-def:EntityObjectStringType	1	1

< rpminfo_state >

The rpminfo_state element defines the different information that can be used to evaluate the specified rpm. This includes the architecture, epoch number, and version numbers. Most of this information can be obtained through the rpm function. Please refer to the individual elements in the schema for more details about what each represents.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-def:EntityStateStringType	0	1
arch	oval-def:EntityStateStringType	0	1
epoch	oval-def:EntityStateStringType	0	1
release	oval-def:EntityStateStringType	0	1
version	oval-def:EntityStateStringType	0	1
evr	oval-def:EntityStateStringType	0	1
signature_keyid	oval-def:EntityStateStringType	0	1