Open Vulnerability and Assessment Language — OVAL®

A Community-Developed Language for Determining Vulnerability and Configuration Issues on Computer Systems

OVAL is an international, information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

The language provides a framework for making assertions about a machine's state by standardizing the three main steps of the assessment process: representing the machine state of a system for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment.

The repositories are collections of publicly available and open content that utilize the language.

OVAL Language

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing machine state, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment. The community has also developed numerous platform-specific component schemas for specifying and representing a system's machine state on those platforms.

OVAL Repository

Content written in the OVAL Language—XML documents such as OVAL Definitions files—is located in the many repositories found within the community. One such repository, the OVAL Repository hosted by The MITRE Corporation, is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

OVAL Adoption

Vendor organizations adopt OVAL by incorporating OVAL into their information security products and services, while users support OVAL by deploying products and services that have adopted OVAL to further enhance the security of their enterprises. A product or service is considered an OVAL Adopter if it uses OVAL as appropriate for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

To be an official OVAL Adopter a product or service must complete the OVAL Adoption Program Process:

- Make a declaration to adopt one or more OVAL Adoption Capabilities.
- Implement the OVAL Adoption Capabilities in the product or service.
- Complete the OVAL Adoption Questionnaire that provides an overview of how the OVAL Adoption Capabilities have been integrated into the product or service.

See the "Requirements and Recommendations for OVAL Adoption and Use" document and the formal OVAL Adoption Program description on the OVAL Web site for details.

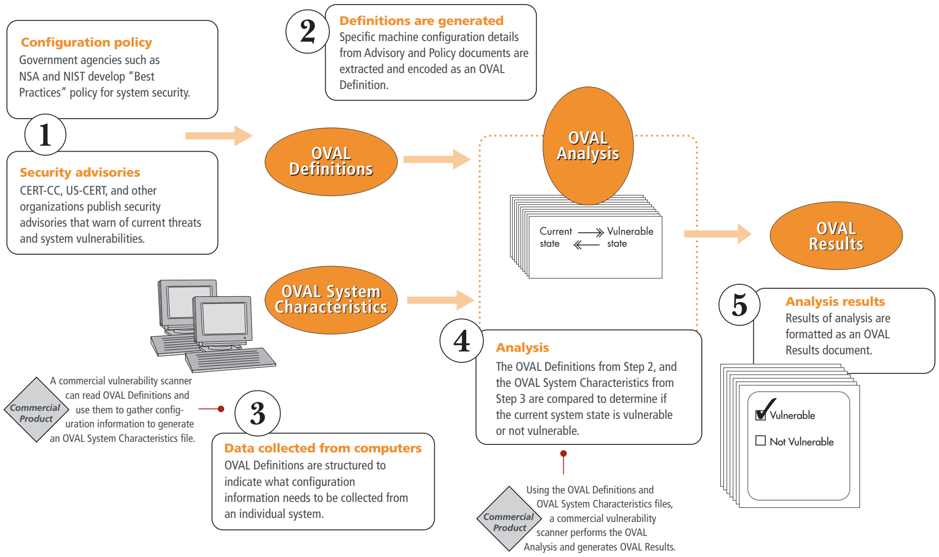
OVAL Community

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developer's Forum and by writing definitions for the OVAL Repository through the OVAL Repository Forum. An OVAL Board consisting of representatives from a broad spectrum of industry

The MITRE Corporation maintains OVAL and its public Web site, manages the adoption program, and provides impartial technical guidance to the OVAL Board and Community throughout the process to ensure OVAL serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org

and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted in the OVAL Repository. This means that OVAL, which is funded by the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.



Configuration policy
Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

Security advisories
CERT-CC, US-CERT, and other organizations publish security advisories that warn of current threats and system vulnerabilities.

Definitions are generated
Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

Data collected from computers
OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

A commercial vulnerability scanner can read OVAL Definitions and use them to gather configuration information to generate an OVAL System Characteristics file.

Analysis
The OVAL Definitions from Step 2, and the OVAL System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not vulnerable.

Using the OVAL Definitions and OVAL System Characteristics files, a commercial vulnerability scanner performs the OVAL Analysis and generates OVAL Results.

Analysis results
Results of analysis are formatted as an OVAL Results document.

How the three core components of the OVAL Language work together during a standard vulnerability assessment process

OVAL Definitions

OVAL Definitions are machine-readable, gold standard tests that definitively determine whether the specified software vulnerability, configuration issue, program, or patch is present on a system. There are four main classes of OVAL Definitions:

OVAL Vulnerability Definitions

Tests that determine the presence of vulnerabilities on systems.

OVAL Compliance Definitions

Tests that determine whether the configuration settings of a system meets a security policy.

OVAL Inventory Definitions

Tests that determine whether a specific piece of software is installed on a system.

OVAL Patch Definitions

Tests that determine whether a particular patch is appropriate for a system.

OVAL Definitions include metadata, a high-level summary, and the detailed definition. Definition metadata provides the OVAL-ID, status of the definition (Draft, Interim, or Accepted), the CVE name or other reference on which the definition (or definitions) is based, the version of the official OVAL Definition Schema the definition works with, a brief description of the security issue covered in the definition, the main author, and a list of the significant contributors to the development of the definition.

The high-level summary includes the following: "Vulnerable software exists," which states the specific operating system (OS), the name of the file with the vulnerability in it, application version, and patch status; and "Vulnerable configuration," which indicates if the service is running or not, specific configuration settings, and workarounds.

The detailed portion of definitions provides the logic for checking for the system characteristics (OS installed, settings in the OS, software applications installed, and settings in applications) to indicate that vulnerable software exists, and configuration attributes (registry key values, file system attributes, and configuration files) to indicate that a vulnerable configuration exists.

Any member of the OVAL Community may submit OVAL Definitions, as detailed on the OVAL Web site. OVAL Content hosted in other OVAL repositories is also often available to the public.

MITRE

Learn More – https://oval.mitre.org