MITRE

# Assessment Summary Results


## Abstract

Assessment Summary Results (ASR) is a proposed open specification for exchanging security assessment results and device inventories of multiple IT assets at the aggregate level. Assessment Summary Results may be thought of as the aggregation specification for Assessment Results Format (ARF). While ARF documents contain very detailed information about few assets, ASR documents contain summarized information about many assets for a single, or limited set of findings. The ASR specification describes how to create ASR instance documents and describes what must be placed in each field for the document to be considered valid. Accompanying XML schemas describe the structure of an ASR instance document and how it should be encoded in XML. ASR is currently managed by the Computer Network Defense Research and Technology Program Management Office (CND R&T PMO), with MITRE performing current development under their direction.


**December, 2010**


**John Wunder, MITRE**
**Jon Baker, MITRE**
**Lieutenant Colonel Joe Wolfkiel, Computer Network Defense Research and Technology Program Management Office**

## Scope

ASR belongs to a suite of specifications that enables the assessment and reporting of IT asset configurations in an enterprise environment, known collectively as configuration automation interfaces. Once completed, the security automation interfaces specifications will describe an end-to-end process for delivering assessment content to sensors and data stores, requesting assessments against that content, reporting on the results of those assessments, and aggregating assessment results to an enterprise level. See the forthcoming security automation interfaces whitepaper for further description of each of the pieces of the suite and how they interact.

The scope of Assessment Summary Results, based on the scope of ARF and the use cases below, is a specification for the format of reporting summarized results for IT security assessments for vulnerabilities, patches, configuration items, platforms, and OVAL/XCCDF results across several assets. The ASR specification also describes how assessment results of different types should be aggregated however it does not include any specification of how results should be collected.

## Technical Use Cases

The following tentative technical use cases for ASR were identified based on current and proposed capabilities for performing high-level reporting at an organizational level.

1. Report the results of an assessment of one or more IT assets against a Security Content Automation Protocol (SCAP)[1] content stream as defined by NIST SP 800-126.
2. Report the results of a device inventory of platforms, configurations, patches, and/or vulnerabilities in the absence of an SCAP content stream for many IT assets.

## Community

The primary implementers of ASR will be assessment tool vendors that produce ASR documents and asset databases, security information managers, or other asset managers that will consume, and potentially re-publish ASR. The end users of these products are the primary drivers behind capabilities and use cases while the product developers themselves are the primary drivers behind technical implementation details.

[1] Per NIST SP 800-126 (Stephen Quinn, David Waltermire, Christopher Johnson, Karen Scarfone, John Banghart): "The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information."

## Format

The ASR specification includes text documentation on how ASR documents must be constructed, XML schema documents describing the format and validation of ASR documents, and a data dictionary that provides detailed explanations about the meaning of each field.

ASR documents may contain information such as a list of assets that were assessed and the corresponding assessment results, counts of assets that meet certain criteria, and groupings of assets based on operational criteria. Assessment results include:

- Vulnerabilities, in the form of CVE[2] lists and assessed state (found, not found, etc)
- Configuration items, in the form of CCE[3] lists and values
- Platforms, in the form of CPE[4] patterns and assessed state
- Patches, in the form of patch identifiers and assessed state
- Assessed state of XCCDF[5] rules or OVAL[6] definitions

## Distribution

ASR has been submitted to NIST as an emerging SCAP specification by CND R&T PMO. MITRE, in coordination with CND R&T PMO, will continue to develop the specification to meet both sponsor requirements and, primarily, the needs of the enterprise reporting community. In particular, MITRE will begin a community involvement effort in order to encourage adoption while updating the specification per community feedback.

## Outreach

MITRE will perform in-person outreach by holding talks at security conferences and hosting sessions at developer days, as well as performing one-on-one interviews with interested parties.

---

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures.
[3] Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues.
[4] Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms, and packages.
[5] The Extensible Configuration Checklist Description Formation (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents.
[6] Open Vulnerability and Assessment Language (OVAL) is an information security community standard to promote open and publically available security content, and to standardize the transfer of this information across security tools and services.

Online, MITRE will host an ASR page on the Making Security Measureable Incubator site. This will point to an Enterprise Reporting mailing list for combined feedback and discussion on ASR, ARF, and PLARR as well as an asr@mitre.org e-mail address for direct feedback to the team.