MITRE

Policy Language for Assessment Results Reporting

Abstract

The Policy Language for Assessment Results Reporting (PLARR) is a proposed specification for use in exchanging SCAP security assessment results among tools in an enterprise environment. PLARR is made up of a technical specification, which describes how to create, exchange, and parse PLARR documents and an XML schema used for representing PLARR documents in a machine-readable format. The expected return of a PLARR document is an Assessment Results Format (ARF) when reporting on few assets or an Assessment Summary Results (ASR) document when reporting aggregate results. PLARR is being developed by MITRE for the Department of Defense Computer Network Defense (CND) Research and Technology PMO and will be submitted to the SCAP community as an emerging specification by MITRE.

December, 2010

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

Scope

PLARR belongs to a suite of specifications that enables the reporting of assessments of IT assets in an enterprise environment, known collectively as security automation interfaces. Once completed, the security automation interfaces specifications will describe an end-to-end process for delivering assessment content to 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 Policy Language for Assessment Results Reporting (PLARR) concept is scoped to include a specification of the definition, expression, and transport of an assessment results policy request. The PLARR definition will include selecting the assets to report on, defining the content that the assets will be assessed against, filtering the results, and aggregating the results. The expression is an XML schema representation of a PLARR request. Transport includes a non-mandatory list of standard interfaces that would allow tools to request and respond to requests for Assessment Results Format (ARF) results. The PLARR specification itself is the definition, expression, and transport described in a prose document.

Technical Use Cases

The primary use cases of PLARR are concerned with transporting assessment results between products in an enterprise environment.

1. An asset manager requests vulnerability, inventory, compliance, and configuration information from an assessment tool. The asset manager is defined as any tool that aggregates information about IT assets from multiple assessment tools, information databases, or scanners. The assessment tool is defined as any tool that can report vulnerability (CVE)[1], inventory (CPE)[2], configuration (CCE)[3], or patch information about any asset.
2. A high-level asset manager (or situational awareness tool) requests aggregate assessment results from lower-level asset managers. Aggregate assessment results contain results from two or more assets aggregated in any manner.

Community

PLARR will be implemented by assessment tool vendors, security information manager vendors, and other security tool vendors that wish to exchange assessment results at either asset or enterprise level. The end users of these tools are the primary drivers for the use cases, while the tool developers themselves are the primary drivers behind technical implementation details.

[1] Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures.

[2] Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms, and packages.

[3] Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues.

Format

The PLARR specification itself will be a text document describing how tools should construct PLARR requests to receive the correct results and how the tool handling the request should construct the resulting ARF results. It will define the sections and data elements of a PLARR request and describe how tools should interpret each one. It will also define a subset of the possible transport interfaces, so that if a tool implements at least one of the interfaces it can ensure interoperability. The PLARR expression will be an XML schema defining how the PLARR request should be represented as XML.

The major sections of a PLARR request are asset population and content specification. Asset population describes how to select which computing assets should be assessed, such as by IP address, region, or owning organization. Content specification describes what the assets should be scanned for, either by directly specifying vulnerabilities, configurations, or platforms to inventory or by passing OVAL[4]/XCCDF[5] (assessment) content directly.

Distribution

The PLARR specification will be submitted, by MITRE, to the SCAP community through the NIST emerging specifications mailing list for comments. Upon finalization and approval, PLARR will be included in the SCAP protocol as an independent SCAP standard. MITRE will be the formal owner of the specification, holding a trademark over it but freely distributing it, as with OVAL. MITRE will also be responsible for evolving the PLARR specification per customer and community feedback and publishing updated versions as required (per project funding).

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.

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

[4] 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.

[5] The Extensible Configuration Checklist Description Formation (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents.