



Standardizing Vulnerabilities

VULNERABILITY MANAGEMENT

Standardizing Vulnerabilities

- Vulnerability management used to be performed by numerous different types of software with no common protocol
- Security Content Automation Protocol (SCAP) led by NIST standardized vulnerability management between different software

<https://scap.nist.gov>

NIST SP 800-117
Guide to Adopting and Using the SCAP



SCAP

- Common Configuration Enumeration (CCE)
 - Standard names for system configuration issues
- Common Platform Enumeration (CPE)
 - Standard names for product names and versions
- Common Vulnerabilities and Exposures (CVE)
 - Standard names for security-related software flaws
- Common Vulnerability Scoring System (CVSS)
 - Standard approach for severity of software flaws



SCAP

- Extensible Configuration Checklist Description Format (XCCDF)
 - Language for checklists and reporting results
- Open Vulnerability and Assessment Language (OVAL)
 - Language for low-level testing procedures used by the checklists

