Security Content Metadata Model with an Efficient Search Methodology for Real Time Monitoring and Threat Intelligence

Preeti Subramanian
<spreeti@secpod.com>
Who am I?

Preeti Subramanian from

working as Software Architect at secPod
Roadmap

- Issues in datasets used by security products
- SCAP and other standards
- What is Metadata Model?
- How to use this metadata?
- Real Time Monitoring and Threat Intelligence
Why is there a lack of commonality or inter-relationship between data sets of different security products?
Why don’t these products talk to each other and devise a response mechanism which works like a single system?
Threat Intelligence

- Malware Attribute Enumeration and Characterization (MAEC)
- Cyber Observables (CybOX)
- Structured Threat Information (STIX)
- Threat Information Exchange (TAXII)
Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.

Searching Metadata

CVE-2015-1483
Symantec NetBackup OpsCenter 7.6.0.2 through 7.6.1 on Linux and UNIX allows remote attackers to execute arbitrary JavaScript code via unspecified vectors.

CVE-2014-2130
Cisco Secure Access Control Server (ACS) provides an unintentional administration web interface based on Apache Tomcat, which allows remote authenticated users to modify application files and configuration files, and consequently execute arbitrary code, by leveraging administrative privileges, aka Bug ID CSCuj83189.

CVE-2015-2218
Multiple cross-site scripting (XSS) vulnerabilities in the wp_ajax_save_item function in wonderpluginaudio.php in the WonderPlugin Audio Player plugin before 2.1 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) item[name] or (2) item[customcss] parameter in a wonderplugin_audio_save_item action to wp-admin/admin-ajax.php or the itemid parameter in the (3) won ...

CVE-2015-2220
Multiple cross-site scripting (XSS) vulnerabilities in the Ninja Forms plugin before 2.8.9 for WordPress allow (1) remote attackers to inject arbitrary web script or HTML via the ninja_forms_field_1 parameter in a ninja_forms_ajax_submit action to wp-admin/admin-ajax.php or (2) remote administrators to inject arbitrary web script or HTML via the fields[1] parameter to wp-admin/post.php.
Details of a CVE

CVE

CVE-2015-0310

Date: (C)2015-01-27  (M)2015-02-24

CVSS Score: 10.0
Exploitability Subscore: 10.0
Impact Subscore: 10.0

Access Vector: NETWORK
Access Complexity: LOW
Authentication: NONE
Confidentiality: COMPLETE
Integrity: COMPLETE
Availability: COMPLETE

Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.

Reference:
Relationship between SCAP entities

CVE-2015-0310

Date: (C)2015-01-27 (M)2015-02-24

CVSS Score: 10.0
Exploitability Subscore: 10.0
Impact Subscore: 10.0

Access Vector: NETWORK
Access Complexity: LOW
Authentication: NONE
Confidentiality: COMPLETE
Integrity: COMPLETE
Availability: COMPLETE

Adobe Flash Player before 12.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before

CPE 7
cpe:/a:adobe:flash_
cpe:/a:adobe:flash_
cpe:/a:adobe:flash_

CWE 1
CWE-264

OVAL 8
oval:org.secpod.ova
oval:org.secpod.ova
oval:org.secpod.ova
oval:org.secpod.ova
oval:org.secpod.ova
How to use Metadata?
How to use metadata?

Sea of Data
- OVAL
- XCCDF
- CVE
- CWE
- CCE
- CPE
- MAEC
- STIX/TAXII
- CAPEC

System Info
- System Info
- System Info

Facts

Metadata
- SCAP entities
- SCAP entities
- SCAP entities

Analytics
- Association
- Real Time monitoring & Response

Correlation
Flow of Incidence Response

- **Events collection**
  - Collects events from system
  - Collects processes, ports, applications information

- **Incident Identification**
  - Suspicious events are marked as incidents

- **Analytics and Correlation**
  - Products are identified using correlation
  - Vulnerabilities related to products are identified
  - Remediation is identified for the vulnerabilities present and prevents further attacks
Real Time Threat Monitoring using Security Content Metadata Model

Incident Identification
Using Systems Metadata
And MAEC etc.

Correlation using SCAP Metadata

Remediation Identification

Adobe Reader identified using PID
Vulner identified

Remediation Identified using CRE

inj-adbe.exe
Exec with PID

adbe
Demo
Reminder!

Please do not forget to fill the feedback form