Security Automation and the CND Data Strategy

October 2009

Dan Schmidt

Agenda

Security Automation

CND Data Strategy

→ Build-to Architecture/Projects

→ Piloting Activities

Securing the Desktop

- **Over the past 18 months there have been two major initiatives that have changed the landscape of the Secure Desktop:**
    - Security Content Automation Protocol (SCAP)
    - Federal Desktop Core Configuration (FDCC)

  – **In addition OMB has mandated all Federal Agencies to:**
    - Adopt standard security configurations for the Desktop
    - Implement automated enforcement for these configurations.

Security Content Automation Protocol (SCAP)

Standards that enable organizations to

automate compliance,
manage vulnerabilities,
perform security measurement,
host of other Asset, Vulnerability,
and Configuration Management related tasks.

Building a Culture of Compliance

- **Automated Standards Based (SCAP) Tools**
  - Regular and reliable security checking
  - Built on repeatable processes
  - Standard metrics
  - Remediation information
  - Results useful to technicians and management alike

- **Giving Management**
  - Regular, understandable communications
  - Greater understand of risks
  - Real data upon which to make management decisions
  - Ability to provide technical direction

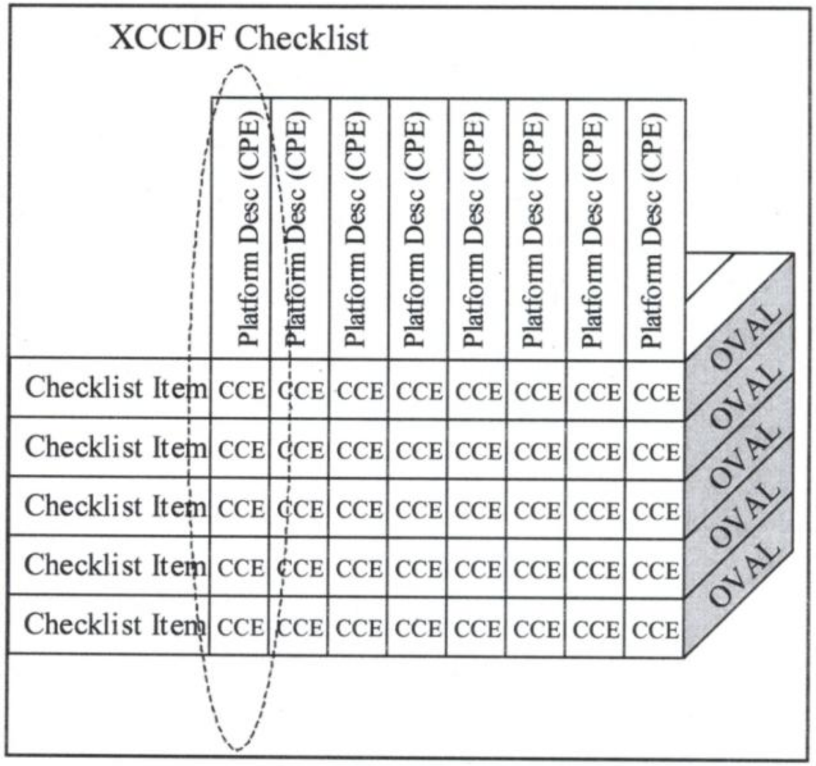
CND Data Strategy

- **Security Standards**
- **Data Models**
- **Architecture**

The objective is to influence existing and future programs

SCAP Standards

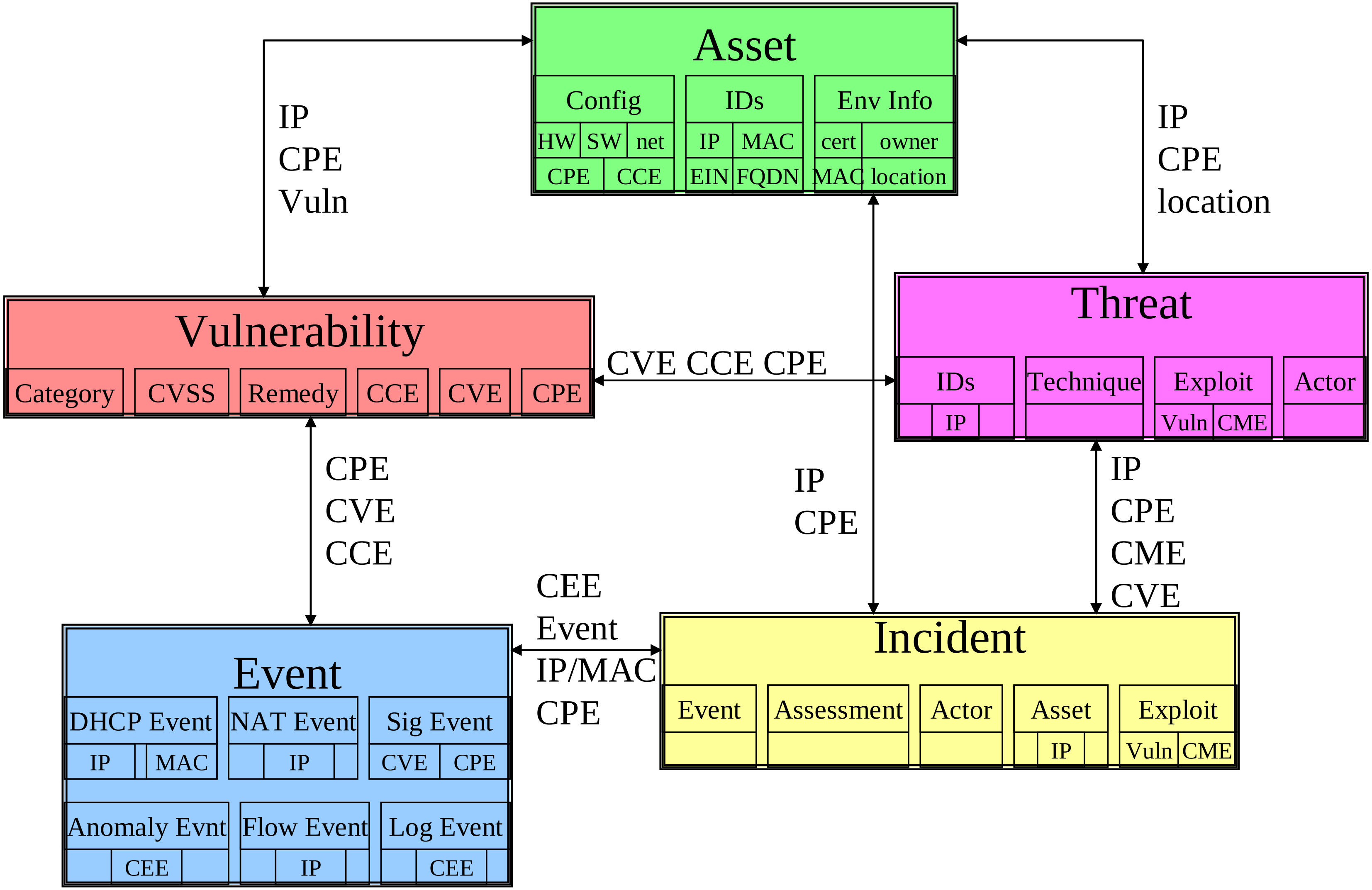
- **OVAL – Language to check for settings and software in a given Operating System**
- **XCCDF – Checklist automation (STIG, Gold Disk, vulnerability checks)**
- **CVE – Standardized IDs for vulnerabilities**
- **CCE – Standardized IDs for settings**
- **CPE – Standardized names for hardware & software**
- **CVSS – Metrics for misconfiguration and vulnerability severity**



XCCDF Checklist

	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	Platform Desc (CPE)	
Checklist Item	CCE	CCE	CCE	CCE	CCE	CCE	CCE	CCE	OVAL
Checklist Item	CCE	CCE	CCE	CCE	CCE	CCE	CCE	CCE	OVAL
Checklist Item	CCE	CCE	CCE	CCE	CCE	CCE	CCE	CCE	OVAL
Checklist Item	CCE	CCE	CCE	CCE	CCE	CCE	CCE	CCE	OVAL
Checklist Item	CCE	CCE	CCE	CCE	CCE	CCE	CCE	CCE	OVAL

CND Data Model Overview



Asset

Config: HW, SW, net, CPE, CCE

IDs: IP, MAC, EIN, FQDN

Env Info: cert, owner, MAC, location

Vulnerability

Category, CVSS, Remedy, CCE, CVE, CPE

Threat

IDs: IP

Technique

Exploit: Vuln, CME

Actor

Event

DHCP Event: IP, MAC

NAT Event: IP

Sig Event: CVE, CPE

Anomaly Evnt: CEE

Flow Event: IP

Log Event: CEE

Incident

Event

Assessment

Actor

Asset: IP

Exploit: Vuln, CME

Asset – Vulnerability: IP, CPE, Vuln

Asset – Threat: IP, CPE, location

Vulnerability – Threat: CVE CCE CPE

Asset – Incident: IP, CPE

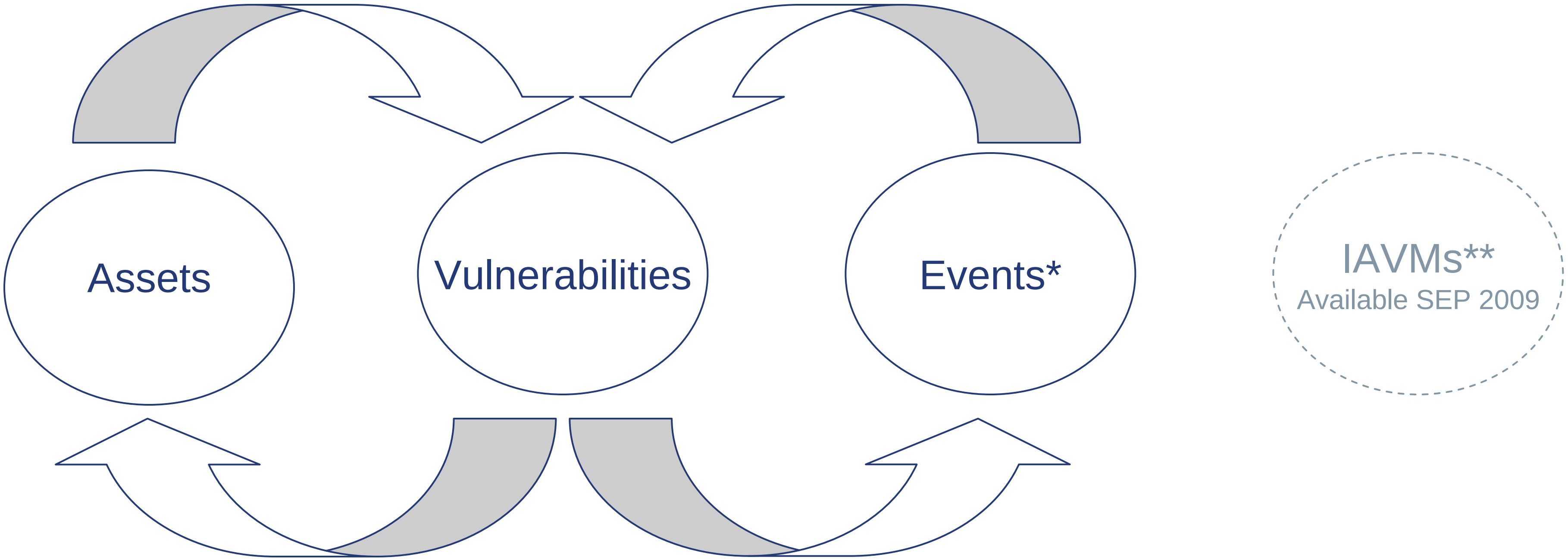
Vulnerability – Event: CPE, CVE, CCE

Threat – Incident: IP, CPE, CME, CVE

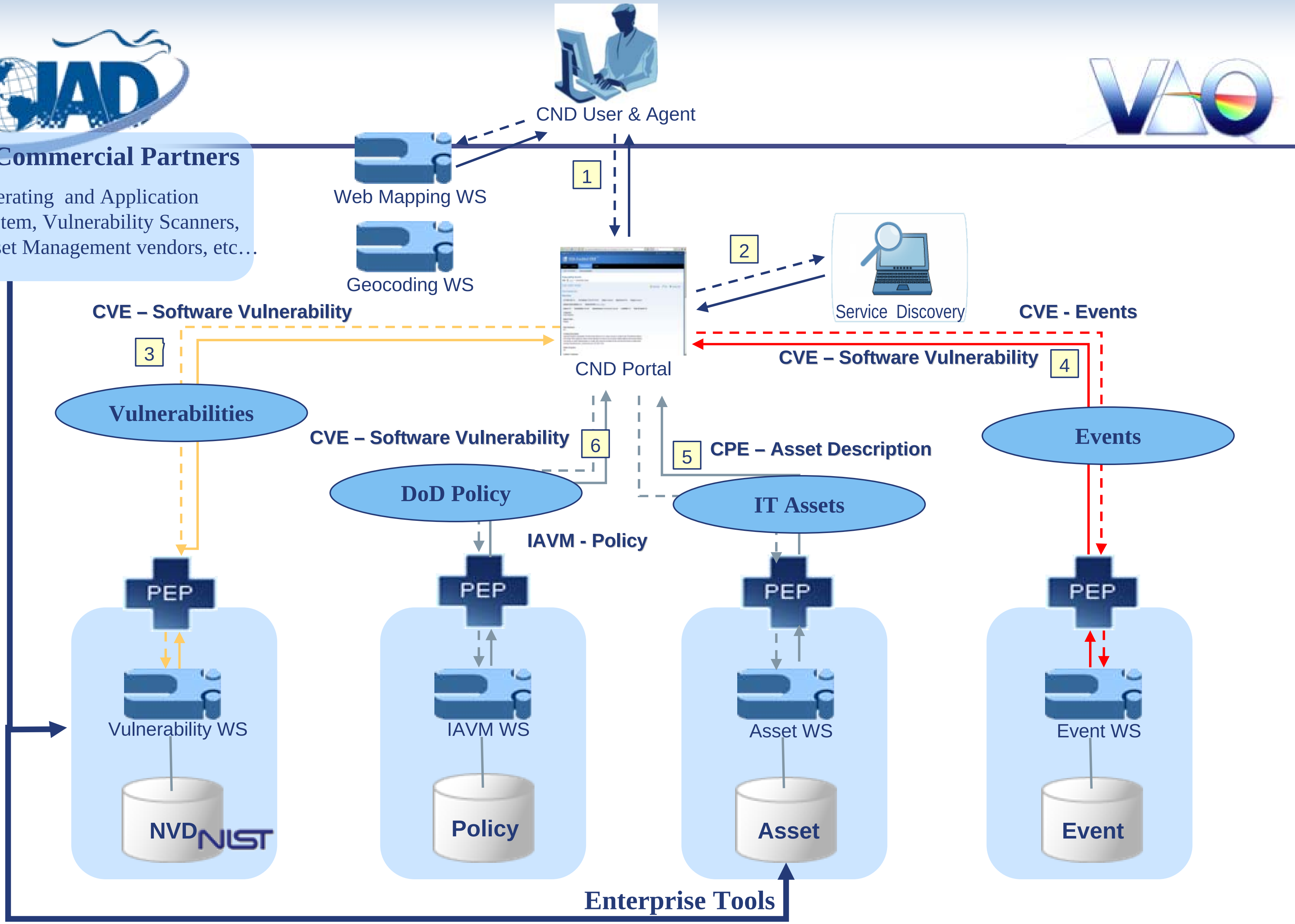
Event – Incident: CEE, Event, IP/MAC, CPE

CND Data Strategy Pilot

Now provides capability to navigate through Assets, Events, and Vulnerabilities as indicated below



*unable to illustrate relating assets directly to events due to only having Events from the Navy and Assets from the Army



CND User & Agent

Web Mapping WS

Geocoding WS

1

2

Service Discovery

CND Portal

3

CVE – Software Vulnerability

CVE - Events

4

CVE – Software Vulnerability

Vulnerabilities

CVE – Software Vulnerability

6

5

CPE – Asset Description

Events

DoD Policy

IT Assets

IAVM - Policy

PEP

PEP

PEP

PEP

Vulnerability WS

IAVM WS

Asset WS

Event WS

NVD NIST

Policy

Asset

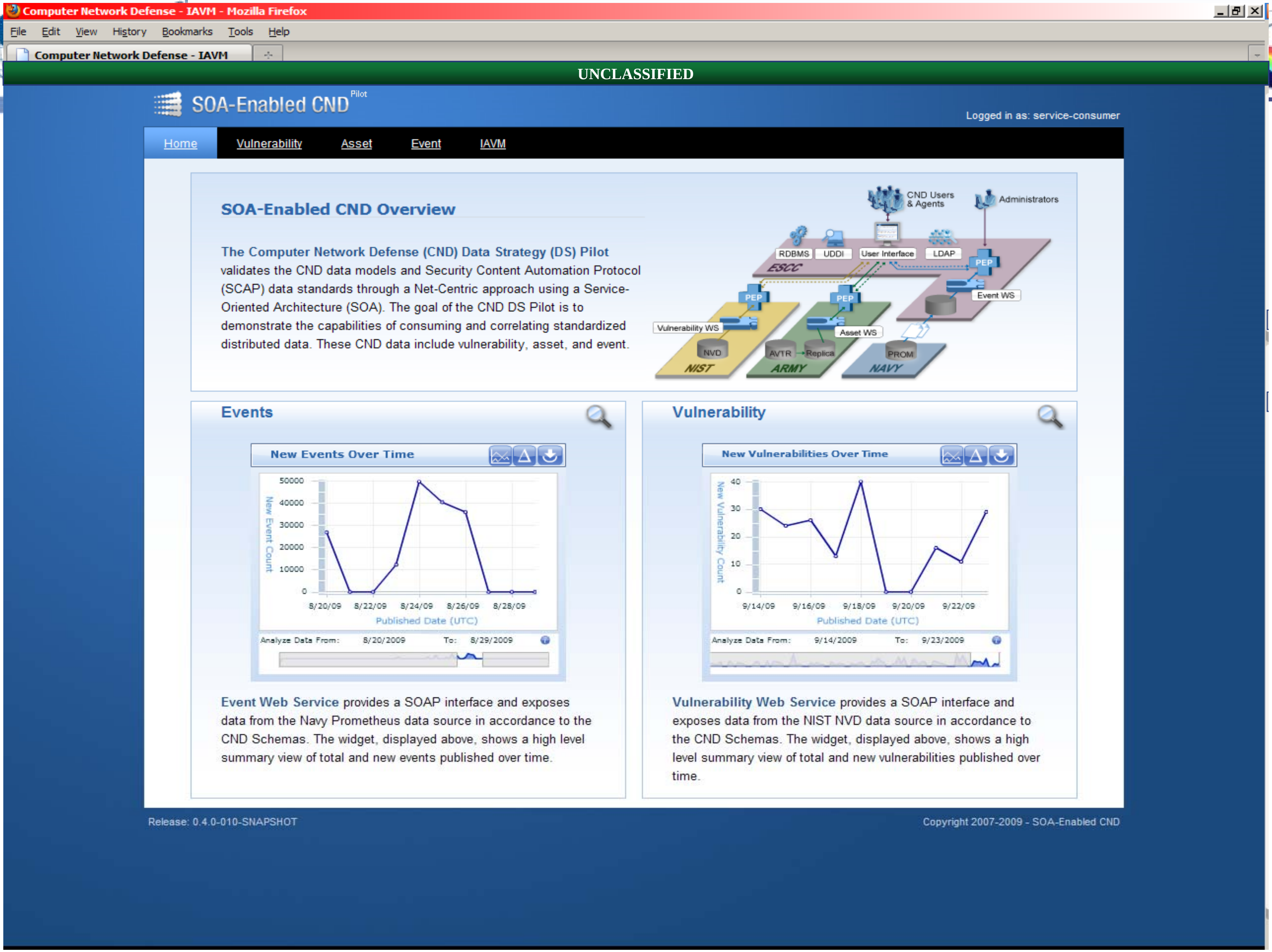
Event

Enterprise Tools

Commercial Partners

Operating and Application System, Vulnerability Scanners, Asset Management vendors, etc…

CND Pilot Home Page



Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM

UNCLASSIFIED

SOA-Enabled CND Pilot

Logged in as: service-consumer

Home
Vulnerability
Asset
Event
IAVM

SOA-Enabled CND Overview

The Computer Network Defense (CND) Data Strategy (DS) Pilot validates the CND data models and Security Content Automation Protocol (SCAP) data standards through a Net-Centric approach using a Service-Oriented Architecture (SOA). The goal of the CND DS Pilot is to demonstrate the capabilities of consuming and correlating standardized distributed data. These CND data include vulnerability, asset, and event.

Events

New Events Over Time

Analyze Data From: 8/20/2009 To: 8/29/2009

Event Web Service provides a SOAP interface and exposes data from the Navy Prometheus data source in accordance to the CND Schemas. The widget, displayed above, shows a high level summary view of total and new events published over time.

Vulnerability

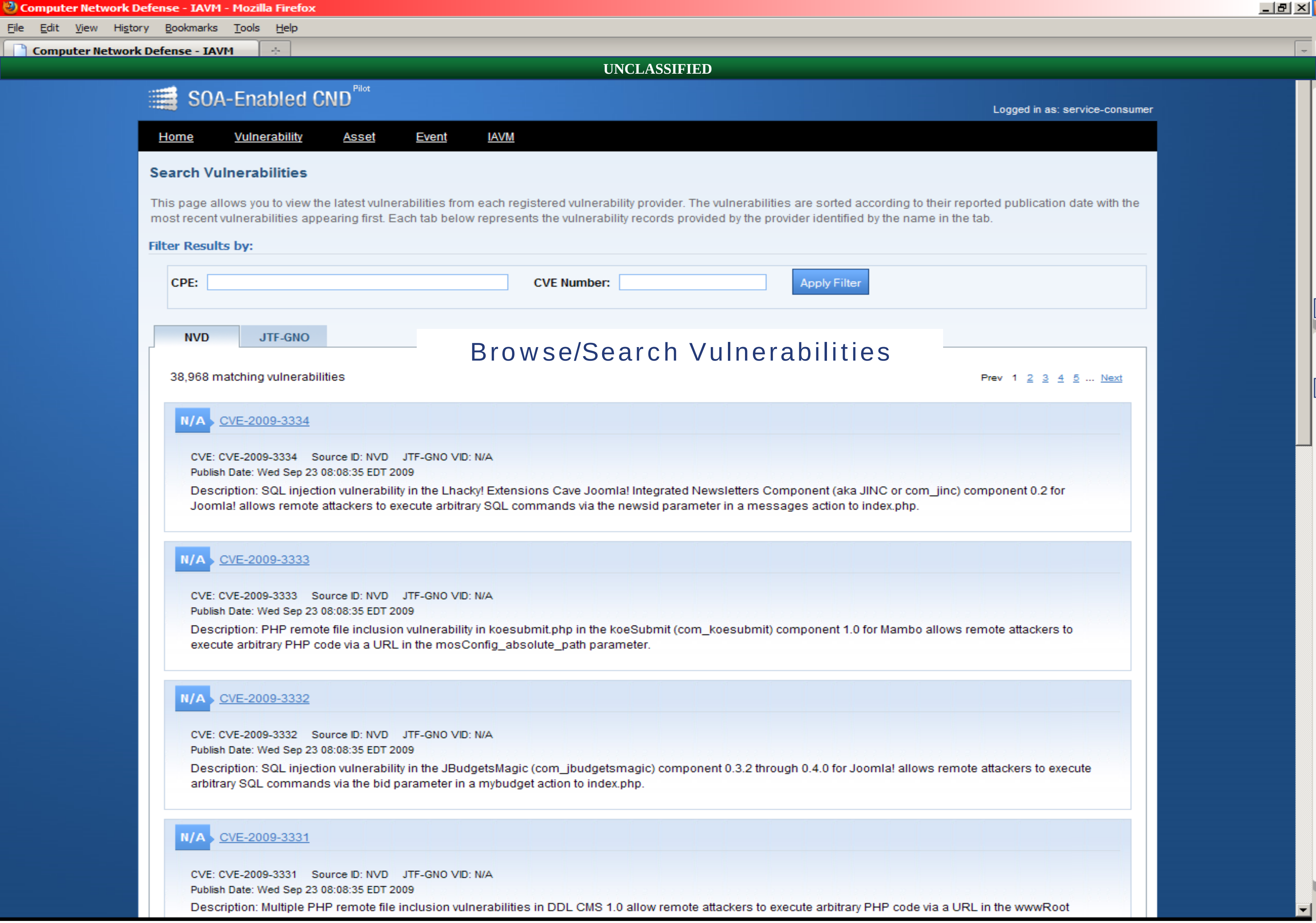
New Vulnerabilities Over Time

Analyze Data From: 9/14/2009 To: 9/23/2009

Vulnerability Web Service provides a SOAP interface and exposes data from the NIST NVD data source in accordance to the CND Schemas. The widget, displayed above, shows a high level summary view of total and new vulnerabilities published over time.

Release: 0.4.0-010-SNAPSHOT

Browse/Search Vulnerabilities


Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM

UNCLASSIFIED

SOA-Enabled CND Pilot

Logged in as: service-consumer

Home Vulnerability Asset Event IAVM

Search Vulnerabilities

This page allows you to view the latest vulnerabilities from each registered vulnerability provider. The vulnerabilities are sorted according to their reported publication date with the most recent vulnerabilities appearing first. Each tab below represents the vulnerability records provided by the provider identified by the name in the tab.

Filter Results by:

CPE: ____ CVE Number: ____ Apply Filter

38,968 matching vulnerabilities

N/A CVE-2009-3334

CVE: CVE-2009-3334 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Wed Sep 23 08:08:35 EDT 2009
Description: SQL injection vulnerability in the Lhacky! Extensions Cave Joomla! Integrated Newsletters Component (aka JINC or com_jinc) component 0.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the newsid parameter in a messages action to index.php.

N/A CVE-2009-3333

CVE: CVE-2009-3333 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Wed Sep 23 08:08:35 EDT 2009
Description: PHP remote file inclusion vulnerability in koesubmit.php in the koeSubmit (com_koesubmit) component 1.0 for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.

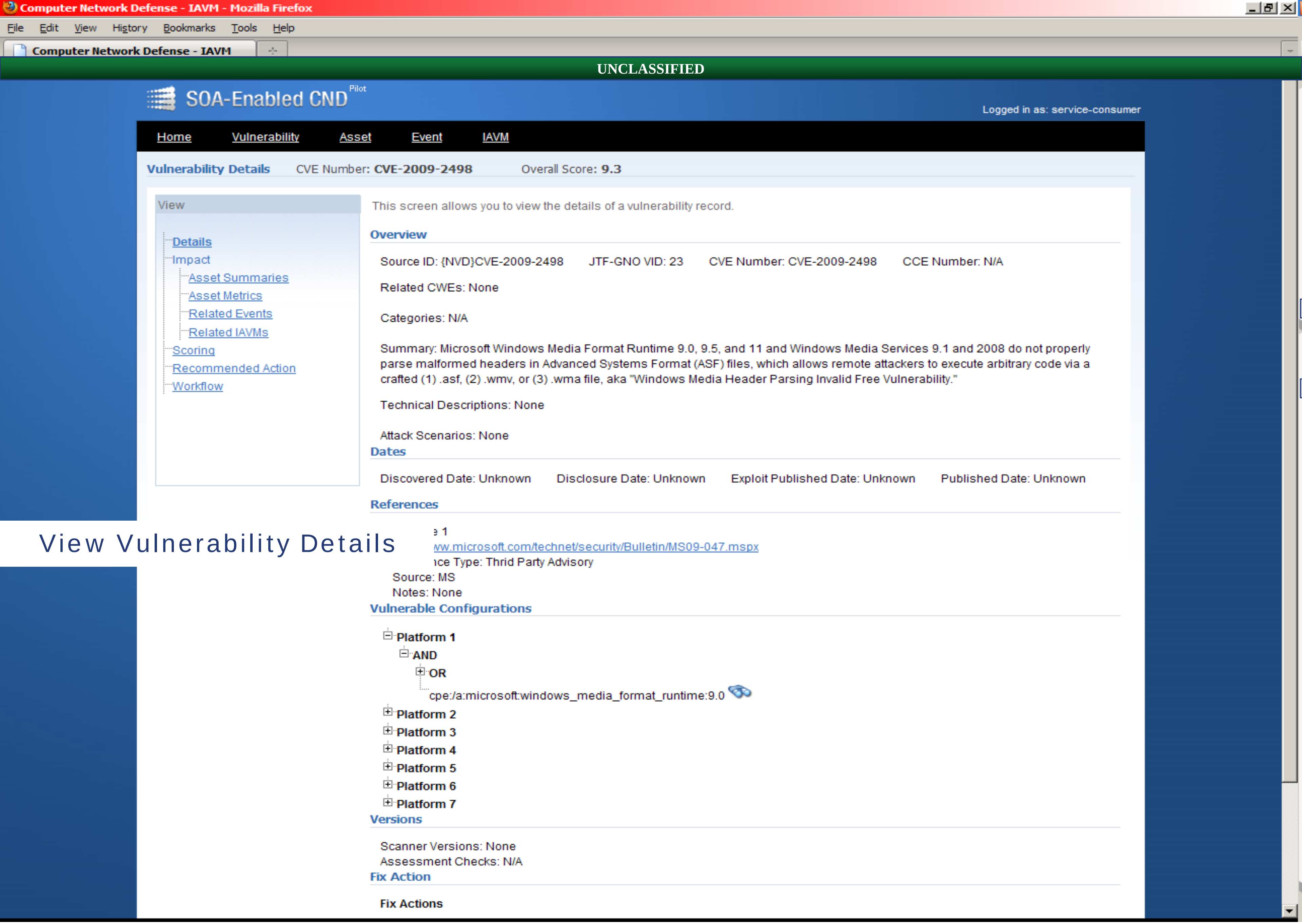
N/A CVE-2009-3332

CVE: CVE-2009-3332 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Wed Sep 23 08:08:35 EDT 2009
Description: SQL injection vulnerability in the JBudgetsMagic (com_jbudgetsmagic) component 0.3.2 through 0.4.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the bid parameter in a mybudget action to index.php.

N/A CVE-2009-3331

CVE: CVE-2009-3331 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Wed Sep 23 08:08:35 EDT 2009
Description: Multiple PHP remote file inclusion vulnerabilities in DDL CMS 1.0 allow remote attackers to execute arbitrary PHP code via a URL in the wwwRoot

View Vulnerability Details



Vulnerability Details CVE Number: **CVE-2009-2498** Overall Score: **9.3**

This screen allows you to view the details of a vulnerability record.

Overview

Source ID: {NVD}CVE-2009-2498 JTF-GNO VID: 23 CVE Number: CVE-2009-2498 CCE Number: N/A

Related CWEs: None

Categories: N/A

Summary: Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka "Windows Media Header Parsing Invalid Free Vulnerability."

Technical Descriptions: None

Attack Scenarios: None

Dates

Discovered Date: Unknown Disclosure Date: Unknown Exploit Published Date: Unknown Published Date: Unknown

References

e 1
ww.microsoft.com/technet/security/Bulletin/MS09-047.mspx
ıce Type: Thrid Party Advisory
Source: MS
Notes: None

Vulnerable Configurations

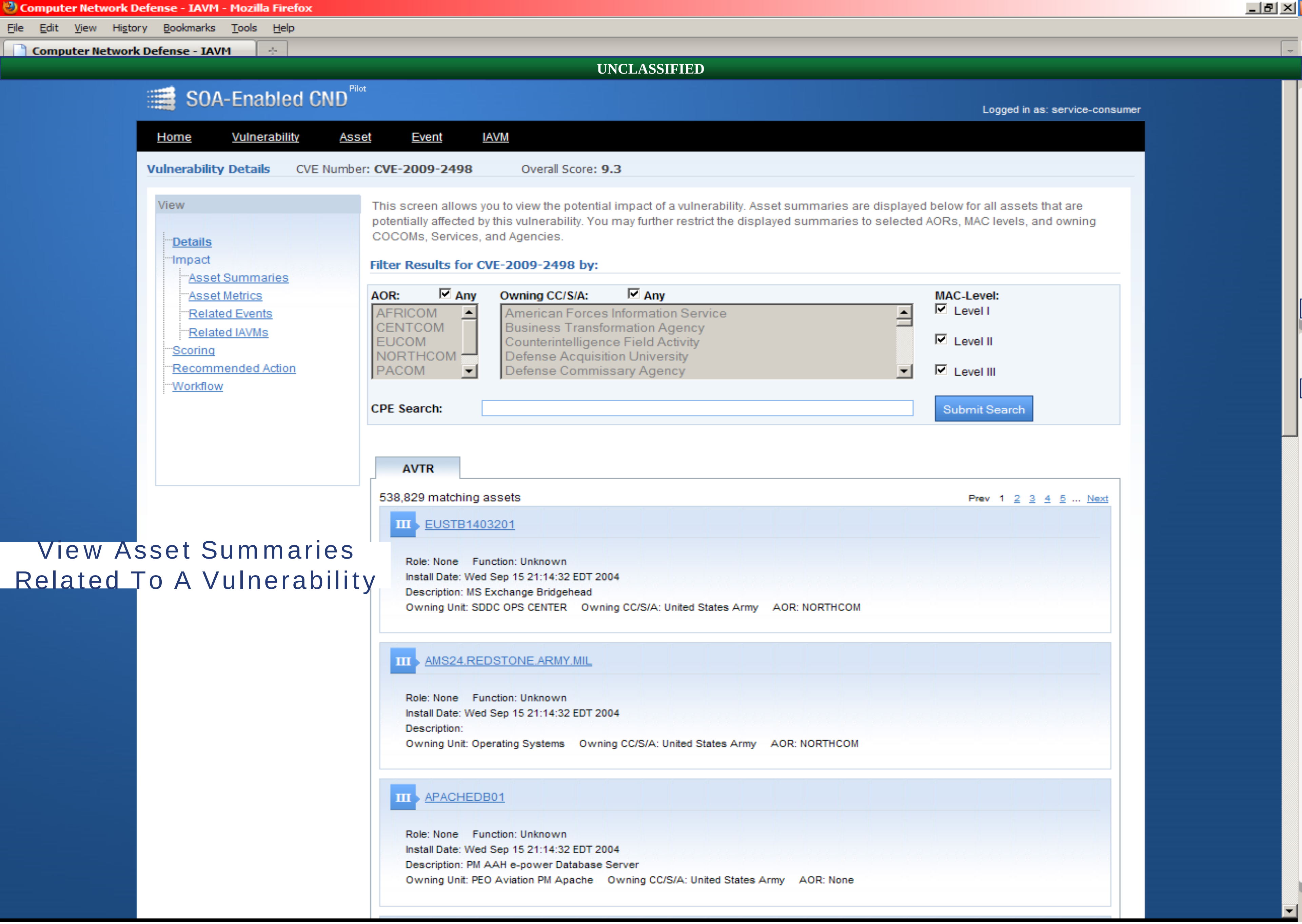
- ⊟ **Platform 1**
  - ⊟ **AND**
    - ⊞ **OR**
    - cpe:/a:microsoft:windows_media_format_runtime:9.0
- ⊞ **Platform 2**
- ⊞ **Platform 3**
- ⊞ **Platform 4**
- ⊞ **Platform 5**
- ⊞ **Platform 6**
- ⊞ **Platform 7**

Versions

Scanner Versions: None
Assessment Checks: N/A

Fix Action

Fix Actions



Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM

UNCLASSIFIED

SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM

Vulnerability Details CVE Number: **CVE-2009-2498** Overall Score: **9.3**

View
Details
Impact
Asset Summaries
Asset Metrics
Related Events
Related IAVMs
Scoring
Recommended Action
Workflow

This screen allows you to view the potential impact of a vulnerability. Asset summaries are displayed below for all assets that are potentially affected by this vulnerability. You may further restrict the displayed summaries to selected AORs, MAC levels, and owning COCOMs, Services, and Agencies.

Filter Results for CVE-2009-2498 by:

AOR: ☑ Any
AFRICOM
CENTCOM
EUCOM
NORTHCOM
PACOM

Owning CC/S/A: ☑ Any
American Forces Information Service
Business Transformation Agency
Counterintelligence Field Activity
Defense Acquisition University
Defense Commissary Agency

MAC-Level:
☑ Level I
☑ Level II
☑ Level III

CPE Search:

538,829 matching assets

III EUSTB1403201

Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description: MS Exchange Bridgehead
Owning Unit: SDDC OPS CENTER Owning CC/S/A: United States Army AOR: NORTHCOM

III AMS24.REDSTONE.ARMY.MIL

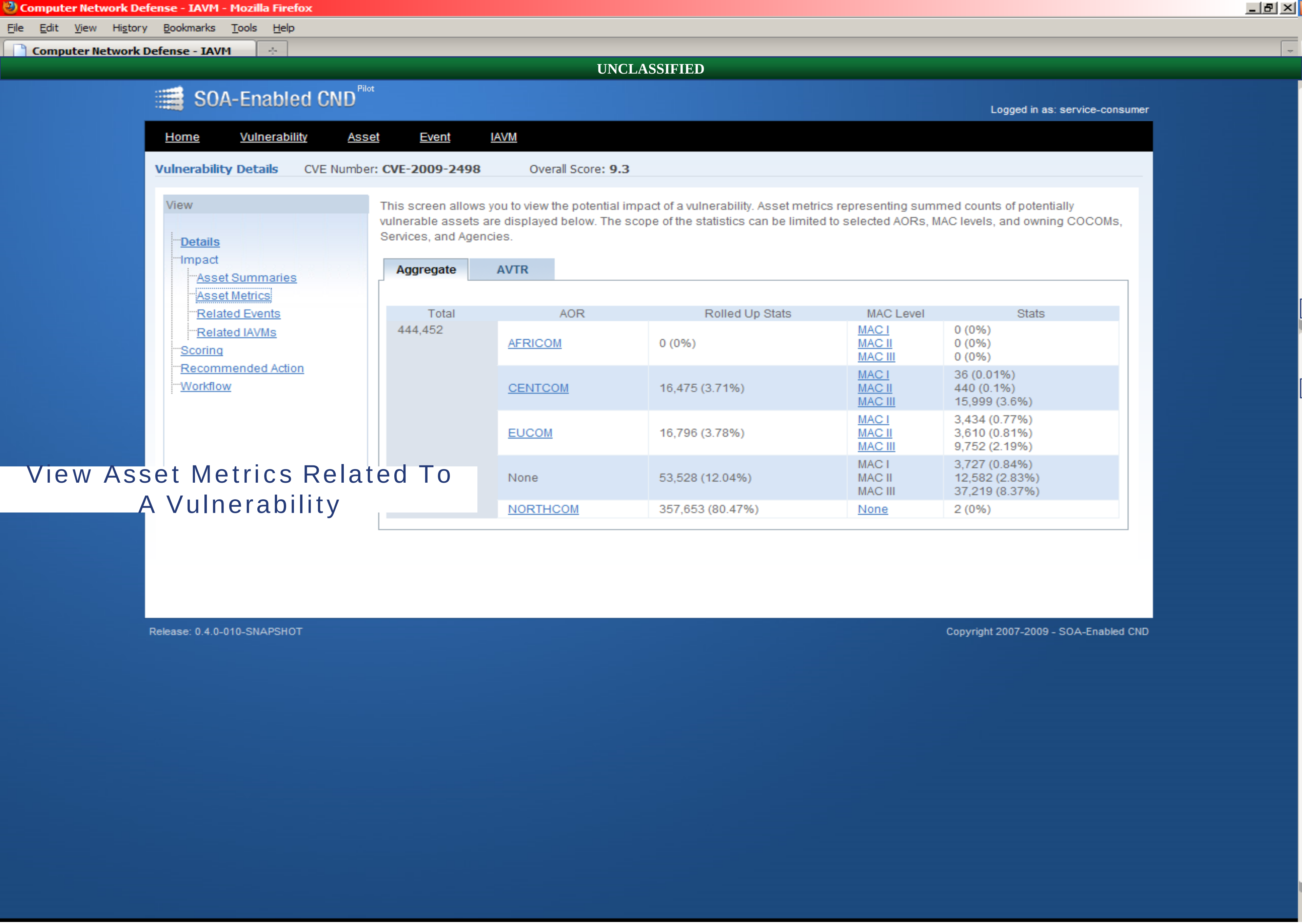
Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description:
Owning Unit: Operating Systems Owning CC/S/A: United States Army AOR: NORTHCOM

III APACHEDB01

Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description: PM AAH e-power Database Server
Owning Unit: PEO Aviation PM Apache Owning CC/S/A: United States Army AOR: None

View Asset Summaries Related To A Vulnerability

View Asset Metrics Related To A Vulnerability



Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM

Vulnerability Details CVE Number: **CVE-2009-2498** Overall Score: **9.3**

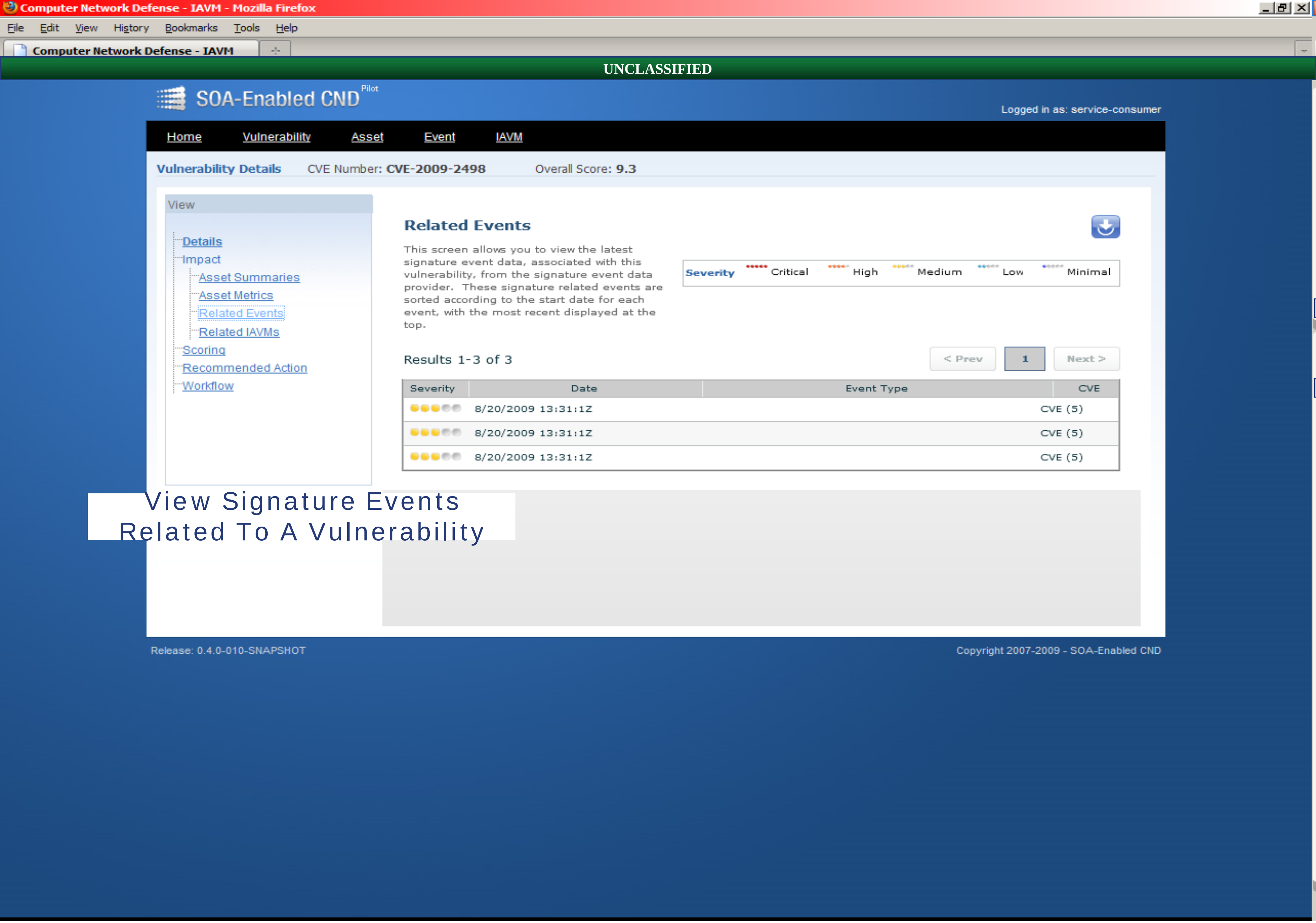
View
Details
Impact
Asset Summaries
Asset Metrics
Related Events
Related IAVMs
Scoring
Recommended Action
Workflow

This screen allows you to view the potential impact of a vulnerability. Asset metrics representing summed counts of potentially vulnerable assets are displayed below. The scope of the statistics can be limited to selected AORs, MAC levels, and owning COCOMs, Services, and Agencies.

Total	AOR	Rolled Up Stats	MAC Level	Stats
444,452	AFRICOM	0 (0%)	MAC I MAC II MAC III	0 (0%) 0 (0%) 0 (0%)
	CENTCOM	16,475 (3.71%)	MAC I MAC II MAC III	36 (0.01%) 440 (0.1%) 15,999 (3.6%)
	EUCOM	16,796 (3.78%)	MAC I MAC II MAC III	3,434 (0.77%) 3,610 (0.81%) 9,752 (2.19%)
	None	53,528 (12.04%)	MAC I MAC II MAC III	3,727 (0.84%) 12,582 (2.83%) 37,219 (8.37%)
	NORTHCOM	357,653 (80.47%)	None	2 (0%)

Release: 0.4.0-010-SNAPSHOT

Copyright 2007-2009 - SOA-Enabled CND



Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM

UNCLASSIFIED

SOA-Enabled CND Pilot

Logged in as: service-consumer

Vulnerability Details CVE Number: **CVE-2009-2498** Overall Score: **9.3**

Related Events

This screen allows you to view the latest signature event data, associated with this vulnerability, from the signature event data provider. These signature related events are sorted according to the start date for each event, with the most recent displayed at the top.

Severity	●●●●● Critical	●●●●○ High	●●●○○ Medium	●●○○○ Low	●○○○○ Minimal

Results 1-3 of 3

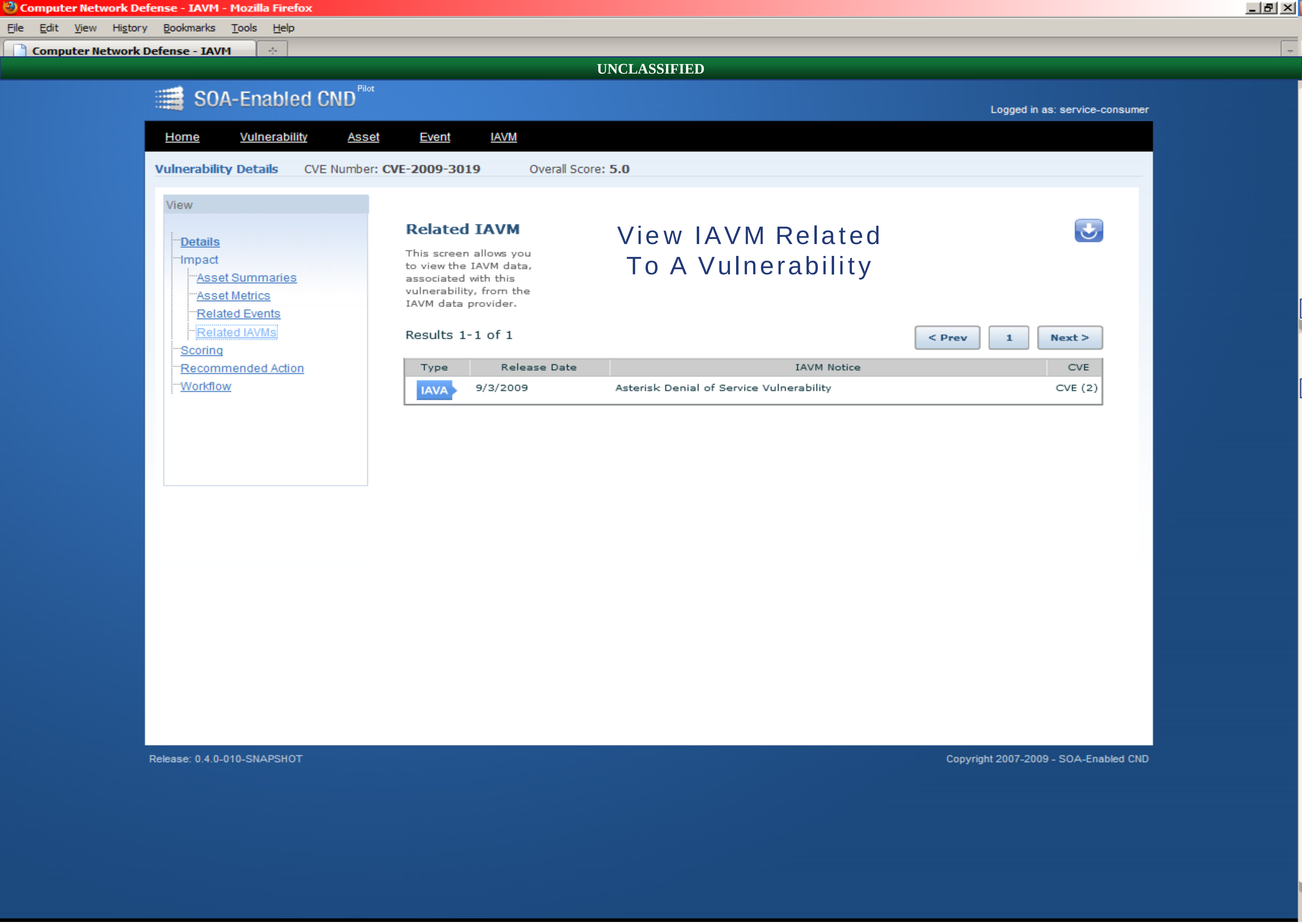
Severity	Date	Event Type	CVE
●●●○○	8/20/2009 13:31:1Z		CVE (5)
●●●○○	8/20/2009 13:31:1Z		CVE (5)
●●●○○	8/20/2009 13:31:1Z		CVE (5)

Release: 0.4.0-010-SNAPSHOT

Copyright 2007-2009 - SOA-Enabled CND

View Signature Events Related To A Vulnerability

View IAVM Related To A Vulnerability



Vulnerability Details CVE Number: **CVE-2009-3019** Overall Score: **5.0**

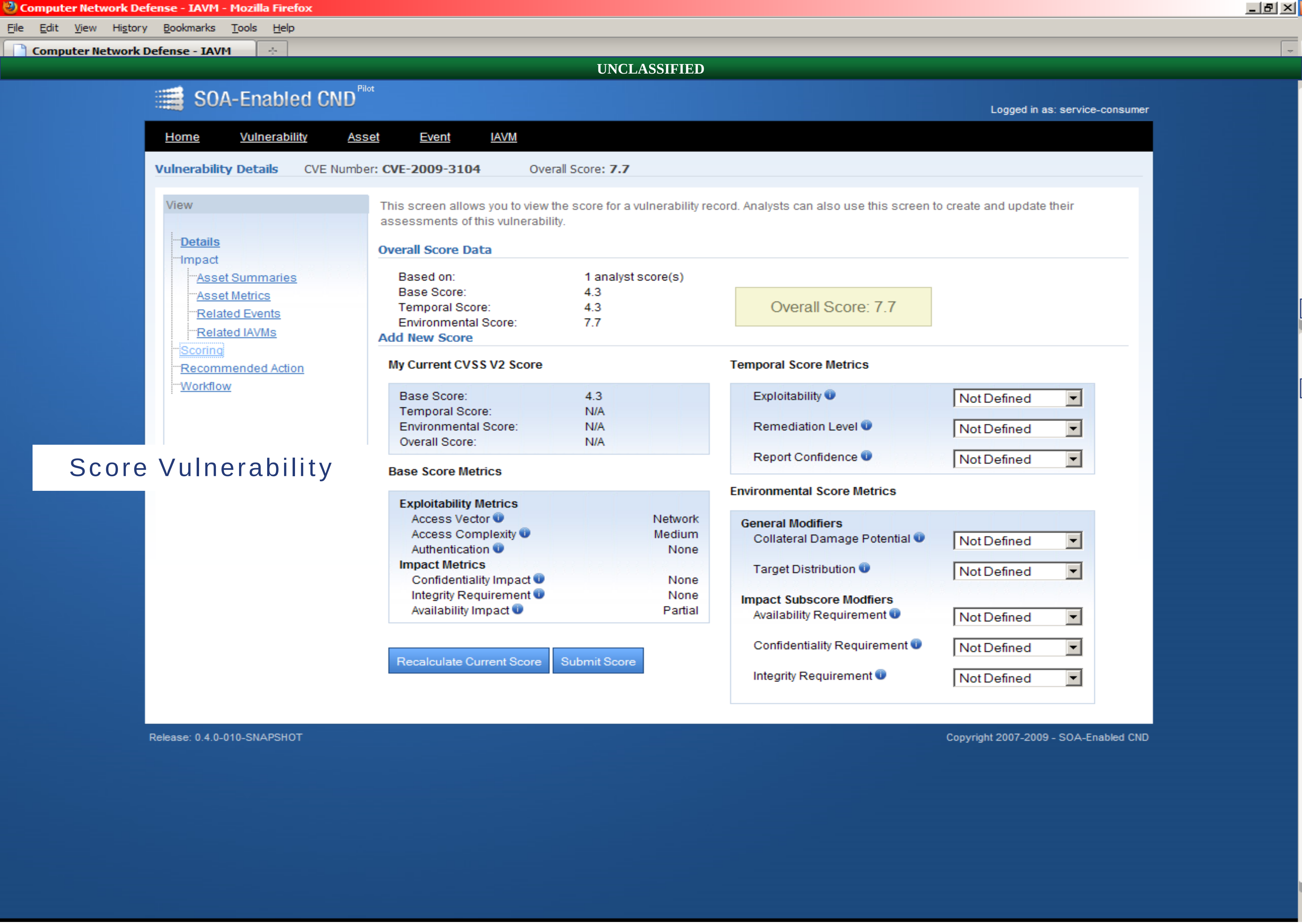
Related IAVM

This screen allows you to view the IAVM data, associated with this vulnerability, from the IAVM data provider.

Results 1-1 of 1

Type	Release Date	IAVM Notice	CVE
IAVA	9/3/2009	Asterisk Denial of Service Vulnerability	CVE (2)

Score Vulnerability



Computer Network Defense - IAVM - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Computer Network Defense - IAVM

UNCLASSIFIED

SOA-Enabled CND Pilot

Logged in as: service-consumer

Home Vulnerability Asset Event IAVM

Vulnerability Details CVE Number: **CVE-2009-3104** Overall Score: **7.7**

View

- Details
- Impact
  - Asset Summaries
  - Asset Metrics
  - Related Events
  - Related IAVMs
- Scoring
- Recommended Action
- Workflow

This screen allows you to view the score for a vulnerability record. Analysts can also use this screen to create and update their assessments of this vulnerability.

Overall Score Data

Based on:	1 analyst score(s)
Base Score:	4.3
Temporal Score:	4.3
Environmental Score:	7.7

Overall Score: 7.7

Add New Score

My Current CVSS V2 Score

Base Score:	4.3
Temporal Score:	N/A
Environmental Score:	N/A
Overall Score:	N/A

Base Score Metrics

Exploitability Metrics	
Access Vector	Network
Access Complexity	Medium
Authentication	None
Impact Metrics	
Confidentiality Impact	None
Integrity Requirement	None
Availability Impact	Partial

Recalculate Current Score Submit Score

Temporal Score Metrics

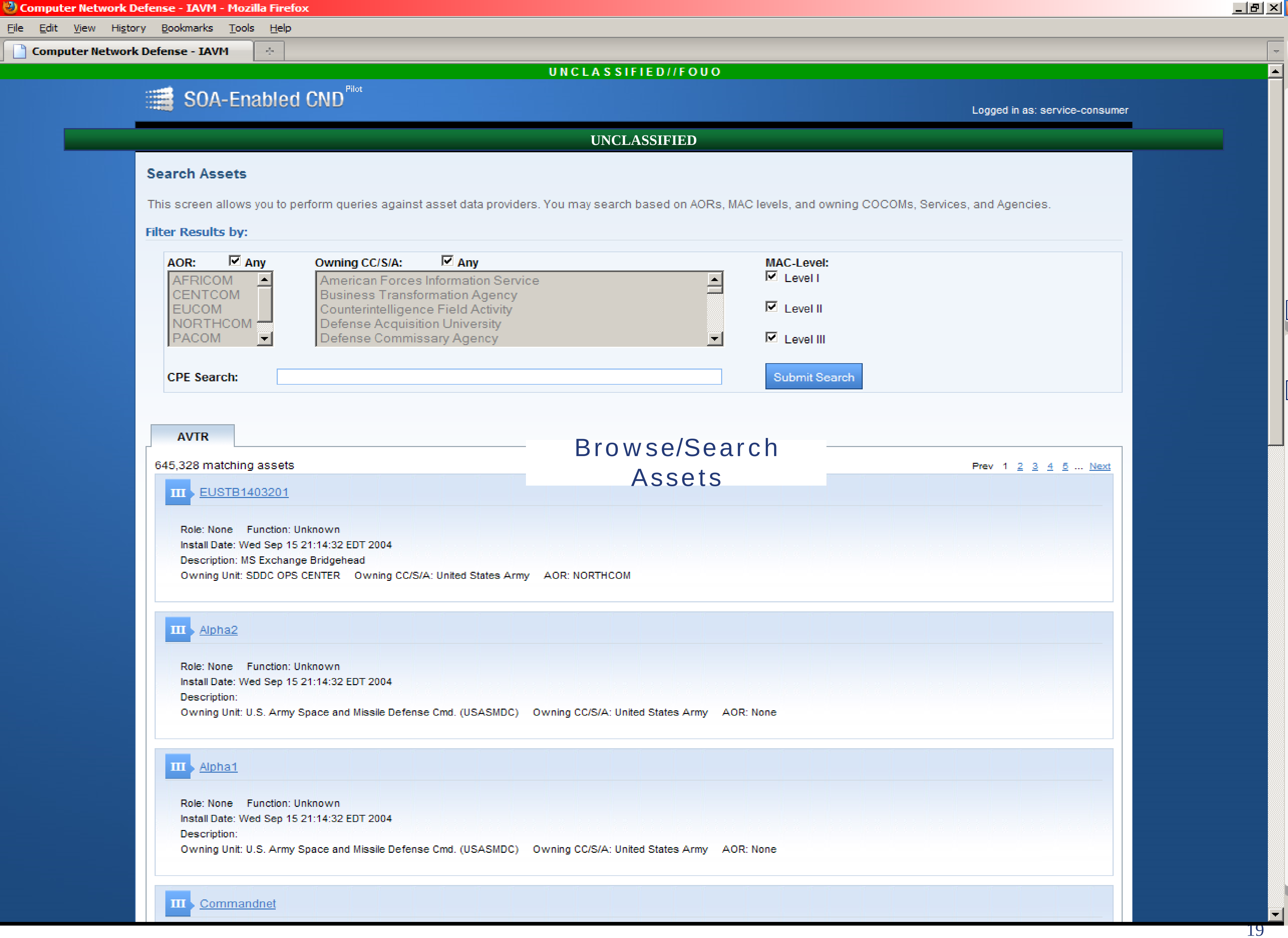
Exploitability	Not Defined
Remediation Level	Not Defined
Report Confidence	Not Defined

Environmental Score Metrics

General Modifiers	
Collateral Damage Potential	Not Defined
Target Distribution	Not Defined
Impact Subscore Modfiers	
Availability Requirement	Not Defined
Confidentiality Requirement	Not Defined
Integrity Requirement	Not Defined

Release: 0.4.0-010-SNAPSHOT

Copyright 2007-2009 - SOA-Enabled CND


Computer Network Defense - IAVM - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Computer Network Defense - IAVM
Submit Search
AVTR

Browse/Search Assets

UNCLASSIFIED//FOUO

SOA-Enabled CND Pilot

Logged in as: service-consumer

UNCLASSIFIED

Search Assets

This screen allows you to perform queries against asset data providers. You may search based on AORs, MAC levels, and owning COCOMs, Services, and Agencies.

Filter Results by:

AOR: ☑ Any
AFRICOM
CENTCOM
EUCOM
NORTHCOM
PACOM

Owning CC/S/A: ☑ Any
American Forces Information Service
Business Transformation Agency
Counterintelligence Field Activity
Defense Acquisition University
Defense Commissary Agency

MAC-Level:
☑ Level I
☑ Level II
☑ Level III

CPE Search:

645,328 matching assets

Prev 1 2 3 4 5 ... Next

III EUSTB1403201

Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description: MS Exchange Bridgehead
Owning Unit: SDDC OPS CENTER Owning CC/S/A: United States Army AOR: NORTHCOM

III Alpha2

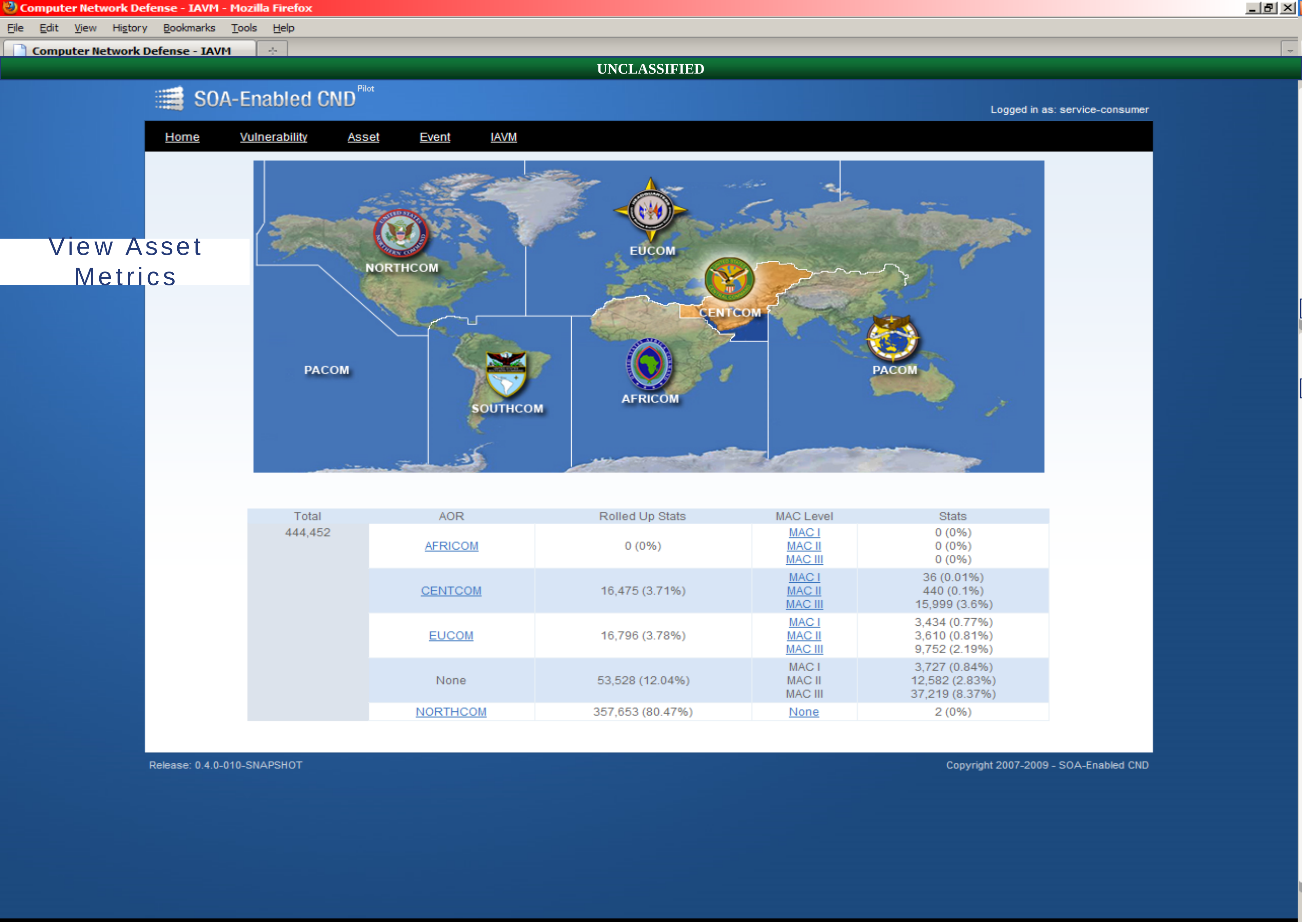
Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description:
Owning Unit: U.S. Army Space and Missile Defense Cmd. (USASMDC) Owning CC/S/A: United States Army AOR: None

III Alpha1

Role: None Function: Unknown
Install Date: Wed Sep 15 21:14:32 EDT 2004
Description:
Owning Unit: U.S. Army Space and Missile Defense Cmd. (USASMDC) Owning CC/S/A: United States Army AOR: None

III Commandnet

View Asset Metrics

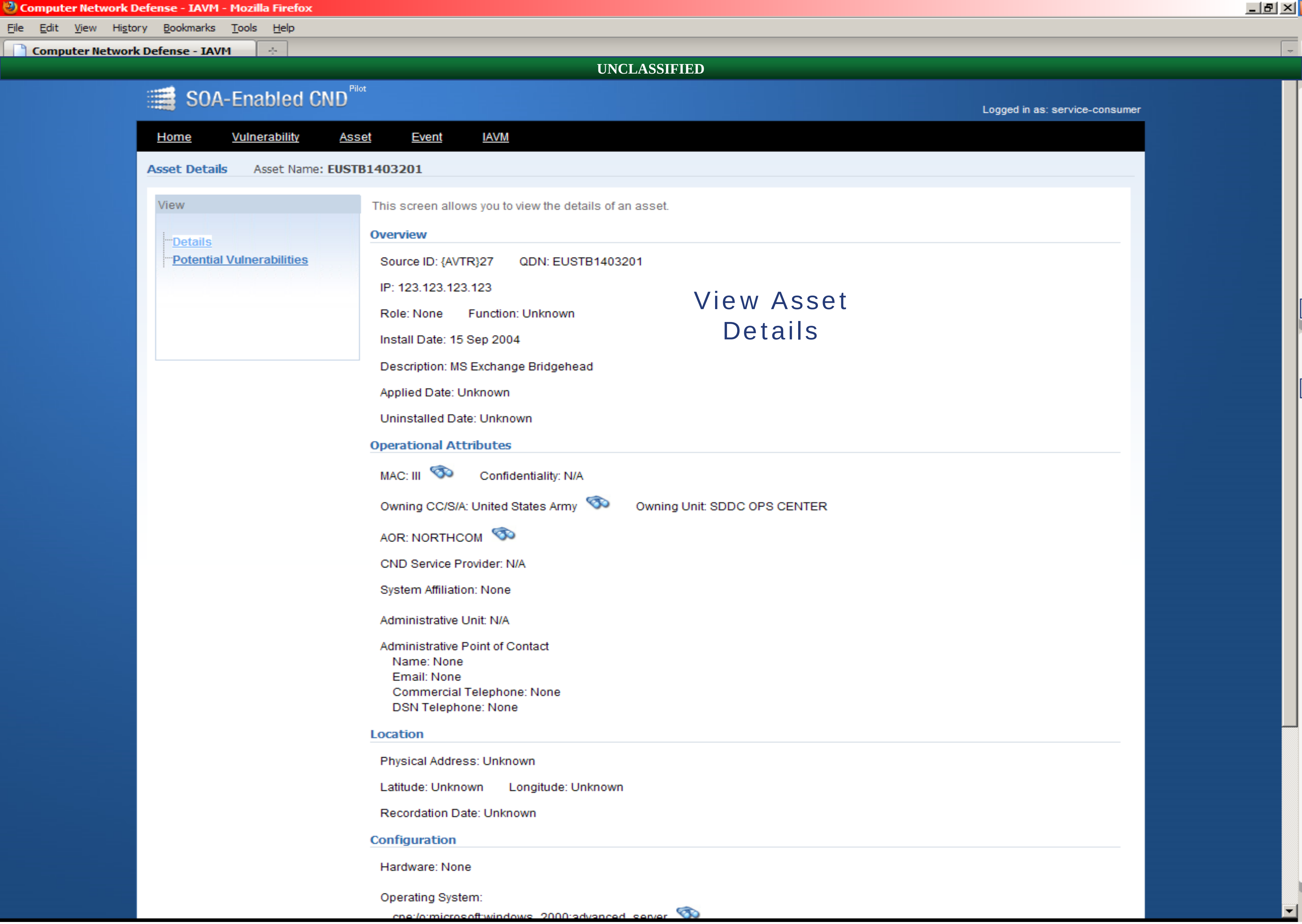

Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM
NORTHCOM
EUCOM
CENTCOM
PACOM
SOUTHCOM
AFRICOM
PACOM

Total	AOR	Rolled Up Stats	MAC Level	Stats
444,452	AFRICOM	0 (0%)	MAC I MAC II MAC III	0 (0%) 0 (0%) 0 (0%)
	CENTCOM	16,475 (3.71%)	MAC I MAC II MAC III	36 (0.01%) 440 (0.1%) 15,999 (3.6%)
	EUCOM	16,796 (3.78%)	MAC I MAC II MAC III	3,434 (0.77%) 3,610 (0.81%) 9,752 (2.19%)
	None	53,528 (12.04%)	MAC I MAC II MAC III	3,727 (0.84%) 12,582 (2.83%) 37,219 (8.37%)
	NORTHCOM	357,653 (80.47%)	None	2 (0%)

Release: 0.4.0-010-SNAPSHOT

Copyright 2007-2009 - SOA-Enabled CND

View Asset Details



Computer Network Defense - IAVM - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home
Vulnerability
Asset
Event
IAVM
View
Details
Potential Vulnerabilities

Asset Details Asset Name: **EUSTB1403201**

This screen allows you to view the details of an asset.

Overview

Source ID: {AVTR}27 QDN: EUSTB1403201

IP: 123.123.123.123

Role: None Function: Unknown

Install Date: 15 Sep 2004

Description: MS Exchange Bridgehead

Applied Date: Unknown

Uninstalled Date: Unknown

Operational Attributes

MAC: III Confidentiality: N/A

Owning CC/S/A: United States Army Owning Unit: SDDC OPS CENTER

AOR: NORTHCOM

CND Service Provider: N/A

System Affiliation: None

Administrative Unit: N/A

Administrative Point of Contact
Name: None
Email: None
Commercial Telephone: None
DSN Telephone: None

Location

Physical Address: Unknown

Latitude: Unknown Longitude: Unknown

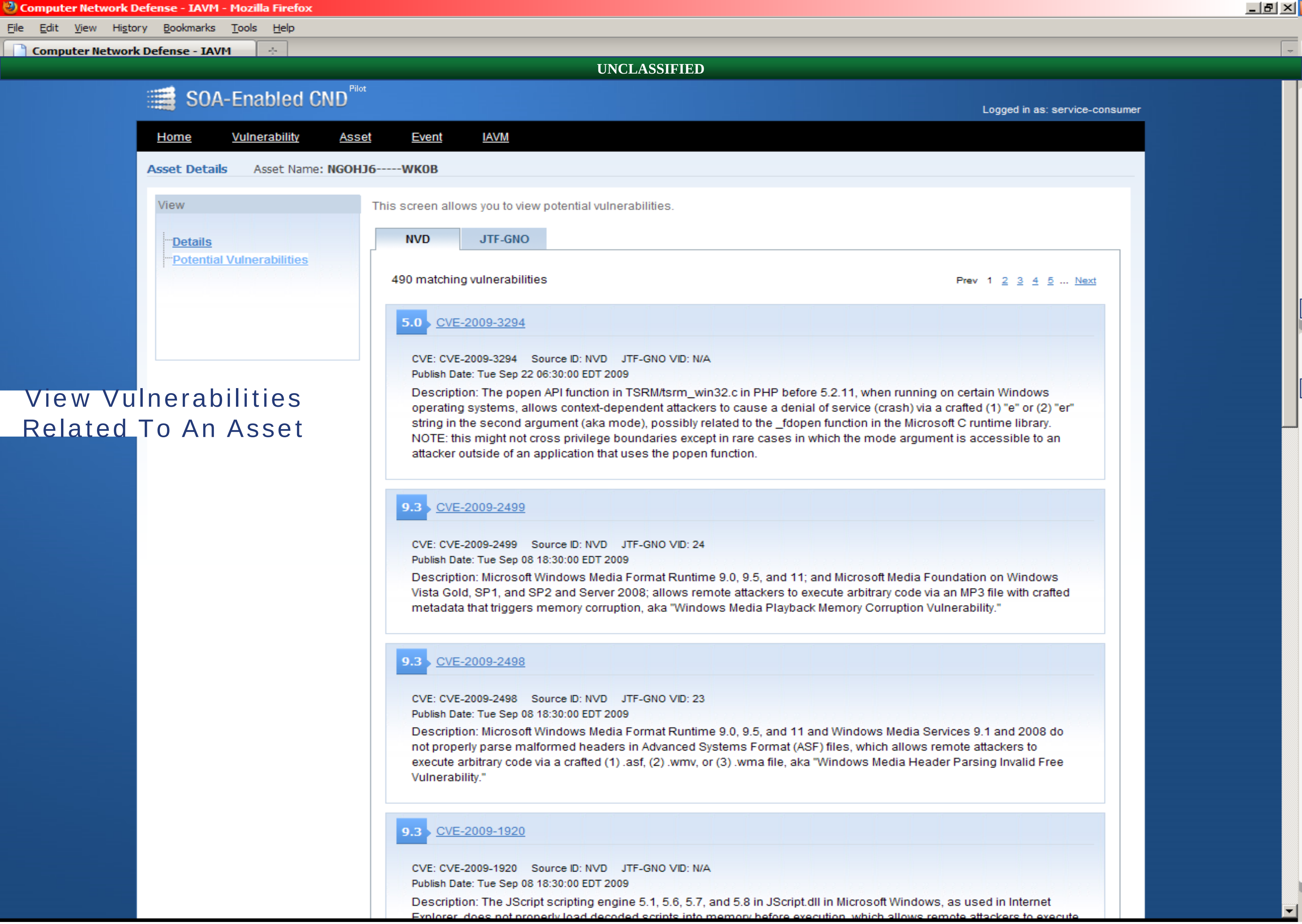
Recordation Date: Unknown

Configuration

Hardware: None

Operating System:
cpe:/o:microsoft:windows_2000:advanced_server

View Vulnerabilities Related To An Asset


Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM
View
Details
Potential Vulnerabilities
NVD
JTF-GNO
Prev 1 2 3 4 5 ... Next

Asset Details Asset Name: NGOHJ6-----WK0B

This screen allows you to view potential vulnerabilities.

490 matching vulnerabilities

5.0 CVE-2009-3294

CVE: CVE-2009-3294 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Tue Sep 22 06:30:00 EDT 2009

Description: The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.

9.3 CVE-2009-2499

CVE: CVE-2009-2499 Source ID: NVD JTF-GNO VID: 24
Publish Date: Tue Sep 08 18:30:00 EDT 2009

Description: Microsoft Windows Media Format Runtime 9.0, 9.5, and 11; and Microsoft Media Foundation on Windows Vista Gold, SP1, and SP2 and Server 2008; allows remote attackers to execute arbitrary code via an MP3 file with crafted metadata that triggers memory corruption, aka "Windows Media Playback Memory Corruption Vulnerability."

9.3 CVE-2009-2498

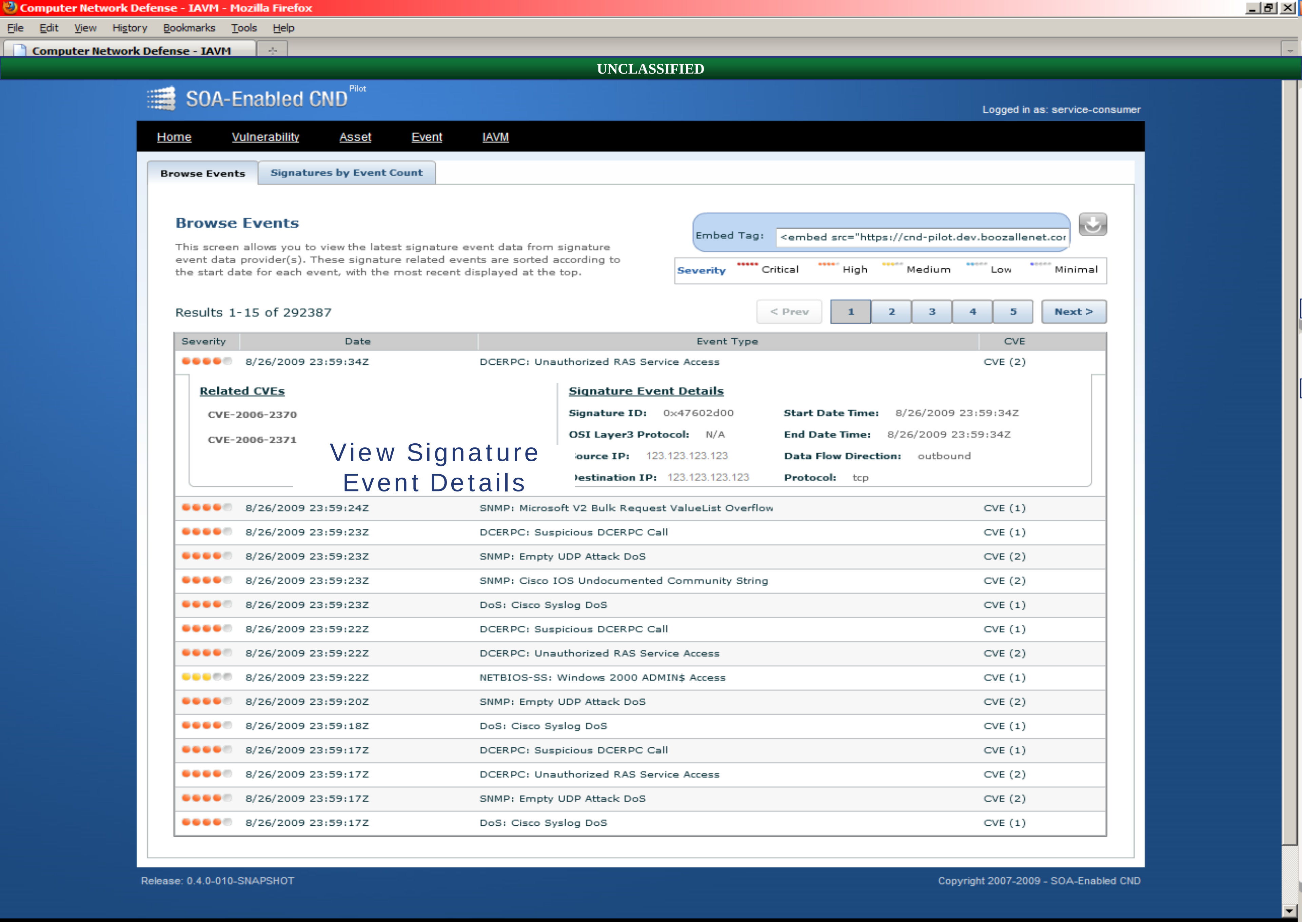
CVE: CVE-2009-2498 Source ID: NVD JTF-GNO VID: 23
Publish Date: Tue Sep 08 18:30:00 EDT 2009

Description: Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka "Windows Media Header Parsing Invalid Free Vulnerability."

9.3 CVE-2009-1920

CVE: CVE-2009-1920 Source ID: NVD JTF-GNO VID: N/A
Publish Date: Tue Sep 08 18:30:00 EDT 2009

Description: The JScript scripting engine 5.1, 5.6, 5.7, and 5.8 in JScript.dll in Microsoft Windows, as used in Internet Explorer, does not properly load decoded scripts into memory before execution, which allows remote attackers to execute


Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM
Browse Events
Signatures by Event Count
< Prev
1 2 3 4 5
Next >

Browse Events

This screen allows you to view the latest signature event data from signature event data provider(s). These signature related events are sorted according to the start date for each event, with the most recent displayed at the top.

Embed Tag: <embed src="https://cnd-pilot.dev.boozallenet.cor

Severity ●●●●● Critical ●●●●○ High ●●●○○ Medium ●●○○○ Low ●○○○○ Minimal

Results 1-15 of 292387

Severity	Date	Event Type	CVE
●●●●○	8/26/2009 23:59:34Z	DCERPC: Unauthorized RAS Service Access	CVE (2)

Related CVEs

CVE-2006-2370

CVE-2006-2371

Signature Event Details

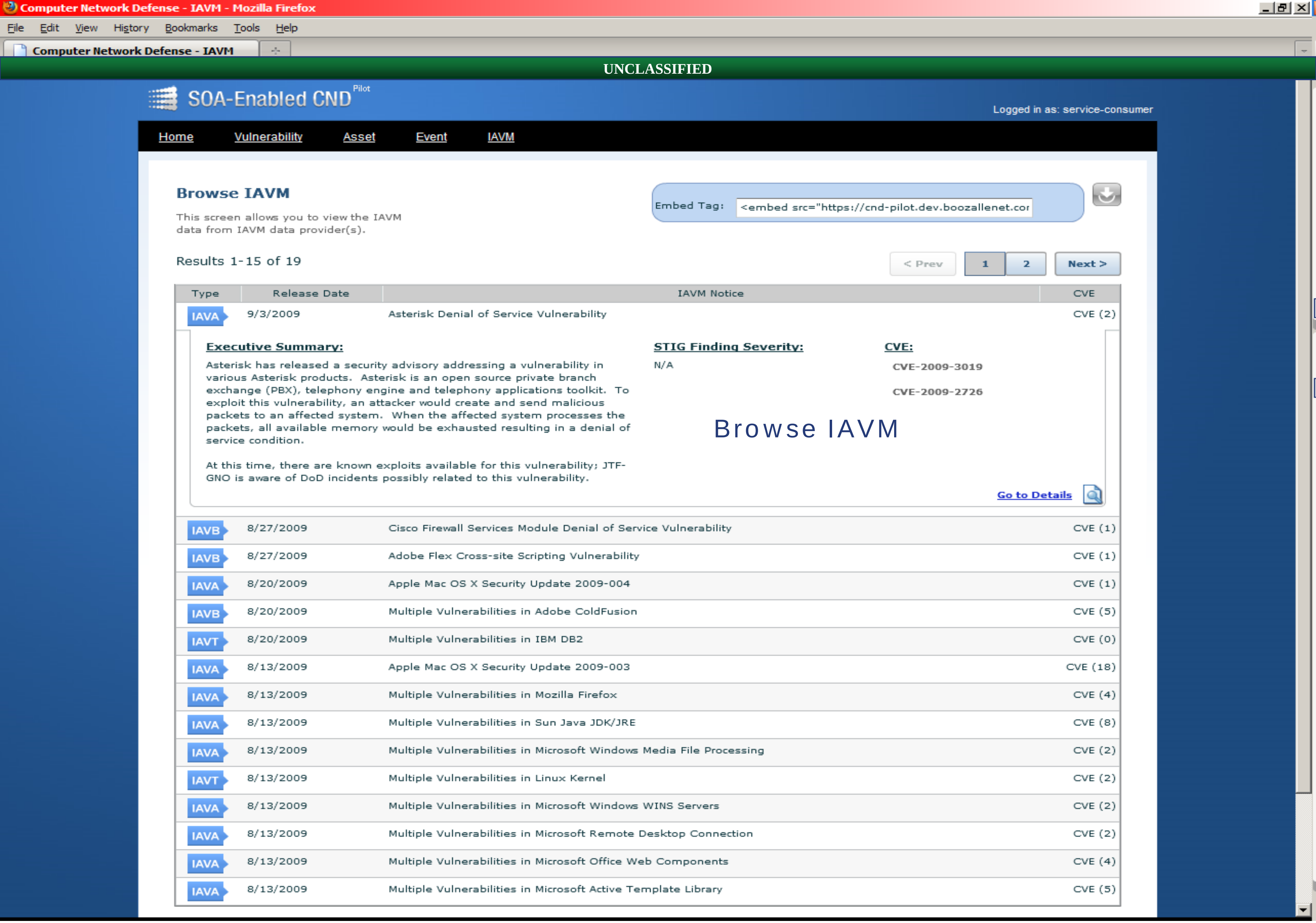
Signature ID:	0x47602d00	**Start Date Time:**	8/26/2009 23:59:34Z
OSI Layer3 Protocol:	N/A	**End Date Time:**	8/26/2009 23:59:34Z
ource IP:	123.123.123.123	**Data Flow Direction:**	outbound
estination IP:	123.123.123.123	**Protocol:**	tcp

View Signature Event Details

Severity	Date	Event Type	CVE
●●●●○	8/26/2009 23:59:24Z	SNMP: Microsoft V2 Bulk Request ValueList Overflow	CVE (1)
●●●●○	8/26/2009 23:59:23Z	DCERPC: Suspicious DCERPC Call	CVE (1)
●●●●○	8/26/2009 23:59:23Z	SNMP: Empty UDP Attack DoS	CVE (2)
●●●●○	8/26/2009 23:59:23Z	SNMP: Cisco IOS Undocumented Community String	CVE (2)
●●●●○	8/26/2009 23:59:23Z	DoS: Cisco Syslog DoS	CVE (1)
●●●●○	8/26/2009 23:59:22Z	DCERPC: Suspicious DCERPC Call	CVE (1)
●●●●○	8/26/2009 23:59:22Z	DCERPC: Unauthorized RAS Service Access	CVE (2)
●●●○○	8/26/2009 23:59:22Z	NETBIOS-SS: Windows 2000 ADMIN$ Access	CVE (1)
●●●●○	8/26/2009 23:59:20Z	SNMP: Empty UDP Attack DoS	CVE (2)
●●●●○	8/26/2009 23:59:18Z	DoS: Cisco Syslog DoS	CVE (1)
●●●●○	8/26/2009 23:59:17Z	DCERPC: Suspicious DCERPC Call	CVE (1)
●●●●○	8/26/2009 23:59:17Z	DCERPC: Unauthorized RAS Service Access	CVE (2)
●●●●○	8/26/2009 23:59:17Z	SNMP: Empty UDP Attack DoS	CVE (2)
●●●●○	8/26/2009 23:59:17Z	DoS: Cisco Syslog DoS	CVE (1)

Release: 0.4.0-010-SNAPSHOT

Copyright 2007-2009 - SOA-Enabled CND



Browse IAVM

Computer Network Defense - IAVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Computer Network Defense - IAVM
UNCLASSIFIED
SOA-Enabled CND Pilot
Logged in as: service-consumer
Home Vulnerability Asset Event IAVM

Browse IAVM

This screen allows you to view the IAVM data from IAVM data provider(s).

Embed Tag: <embed src="https://cnd-pilot.dev.boozallenet.cor

Results 1-15 of 19

Type	Release Date	IAVM Notice	CVE
IAVA	9/3/2009	Asterisk Denial of Service Vulnerability	CVE (2)

Executive Summary:

Asterisk has released a security advisory addressing a vulnerability in various Asterisk products. Asterisk is an open source private branch exchange (PBX), telephony engine and telephony applications toolkit. To exploit this vulnerability, an attacker would create and send malicious packets to an affected system. When the affected system processes the packets, all available memory would be exhausted resulting in a denial of service condition.

At this time, there are known exploits available for this vulnerability; JTF-GNO is aware of DoD incidents possibly related to this vulnerability.

STIG Finding Severity:

N/A

CVE:

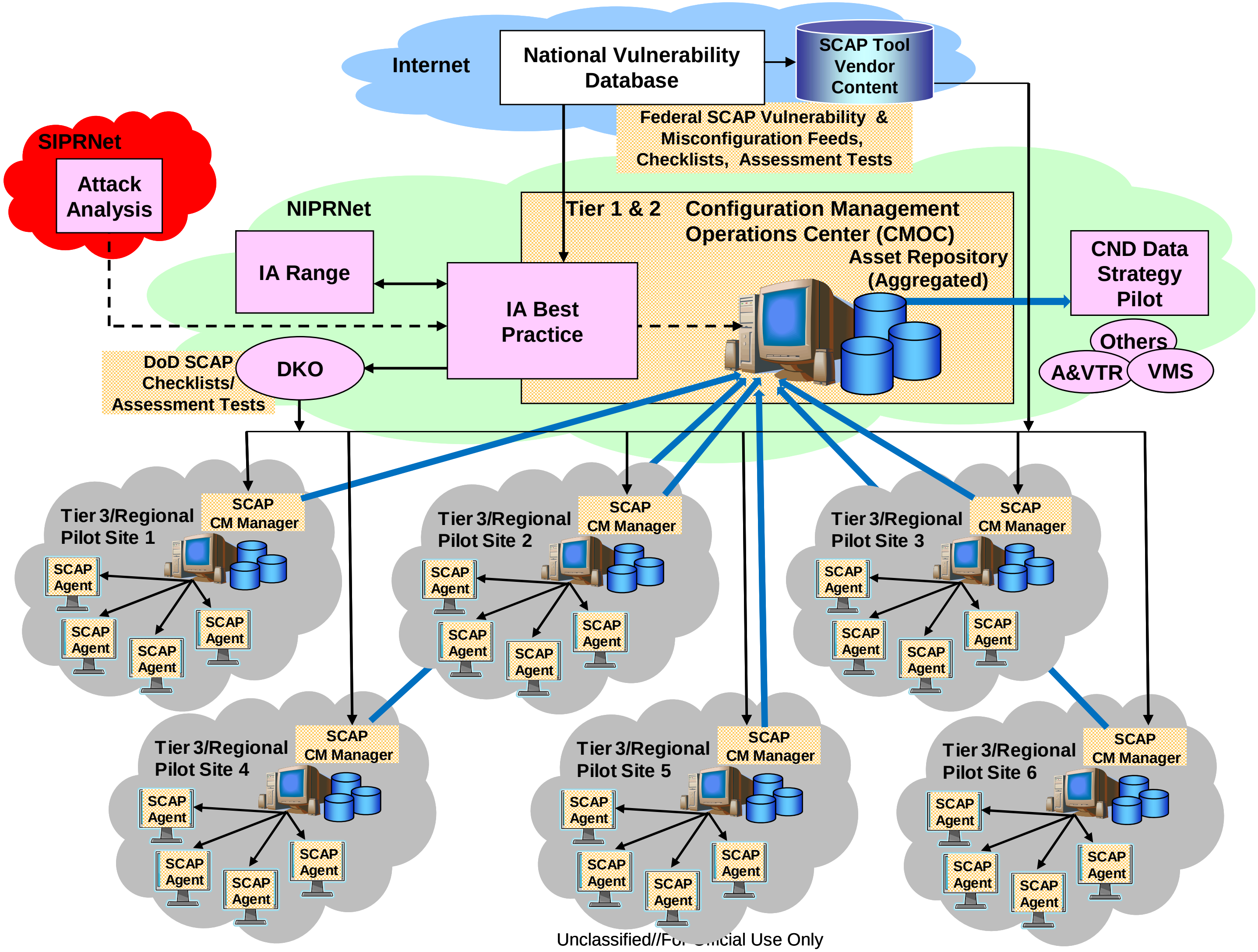
CVE-2009-3019

CVE-2009-2726

Go to Details

Type	Release Date	IAVM Notice	CVE
IAVB	8/27/2009	Cisco Firewall Services Module Denial of Service Vulnerability	CVE (1)
IAVB	8/27/2009	Adobe Flex Cross-site Scripting Vulnerability	CVE (1)
IAVA	8/20/2009	Apple Mac OS X Security Update 2009-004	CVE (1)
IAVB	8/20/2009	Multiple Vulnerabilities in Adobe ColdFusion	CVE (5)
IAVT	8/20/2009	Multiple Vulnerabilities in IBM DB2	CVE (0)
IAVA	8/13/2009	Apple Mac OS X Security Update 2009-003	CVE (18)
IAVA	8/13/2009	Multiple Vulnerabilities in Mozilla Firefox	CVE (4)
IAVA	8/13/2009	Multiple Vulnerabilities in Sun Java JDK/JRE	CVE (8)
IAVA	8/13/2009	Multiple Vulnerabilities in Microsoft Windows Media File Processing	CVE (2)
IAVT	8/13/2009	Multiple Vulnerabilities in Linux Kernel	CVE (2)
IAVA	8/13/2009	Multiple Vulnerabilities in Microsoft Windows WINS Servers	CVE (2)
IAVA	8/13/2009	Multiple Vulnerabilities in Microsoft Remote Desktop Connection	CVE (2)
IAVA	8/13/2009	Multiple Vulnerabilities in Microsoft Office Web Components	CVE (4)
IAVA	8/13/2009	Multiple Vulnerabilities in Microsoft Active Template Library	CVE (5)

(U) Pilot Architecture



Internet

National Vulnerability Database

SCAP Tool Vendor Content

Federal SCAP Vulnerability & Misconfiguration Feeds, Checklists, Assessment Tests

SIPRNet

Attack Analysis

NIPRNet

IA Range

IA Best Practice

Tier 1 & 2 Configuration Management Operations Center (CMOC)

Asset Repository (Aggregated)

CND Data Strategy Pilot

Others

A&VTR

VMS

DoD SCAP Checklists/ Assessment Tests

DKO

Tier 3/Regional Pilot Site 1

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

Tier 3/Regional Pilot Site 2

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

Tier 3/Regional Pilot Site 3

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

Tier 3/Regional Pilot Site 4

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

Tier 3/Regional Pilot Site 5

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

Tier 3/Regional Pilot Site 6

SCAP CM Manager

SCAP Agent

SCAP Agent

SCAP Agent

SCAP Agent

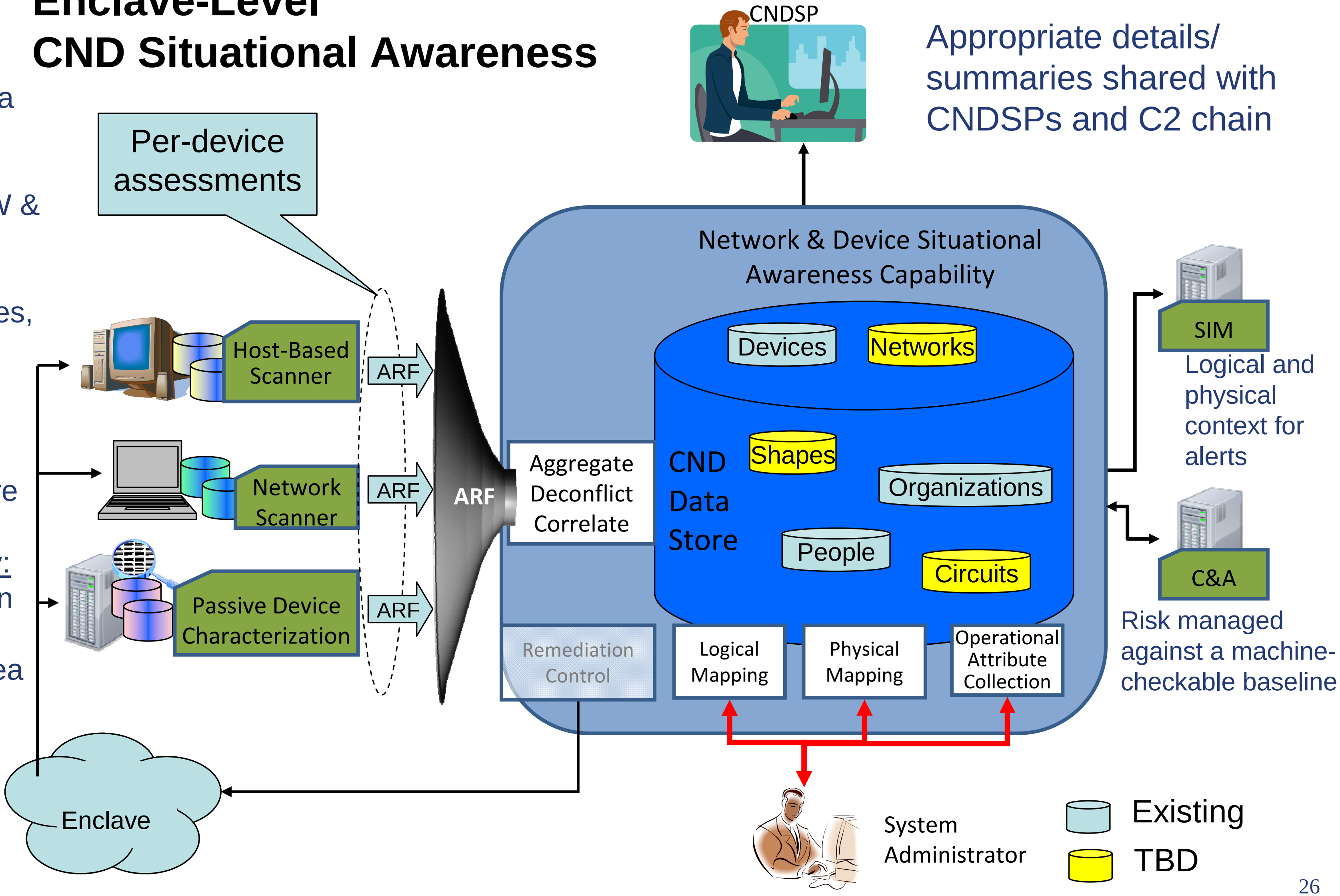
Enclave-Level CND Situational Awareness

Reports - on a per-device basis of:

- Installed SW & HW
- Patches, vulnerabilities, settings
- Running services
- Network infrastructure

Organized by:

- Organization
- Network
- Physical area

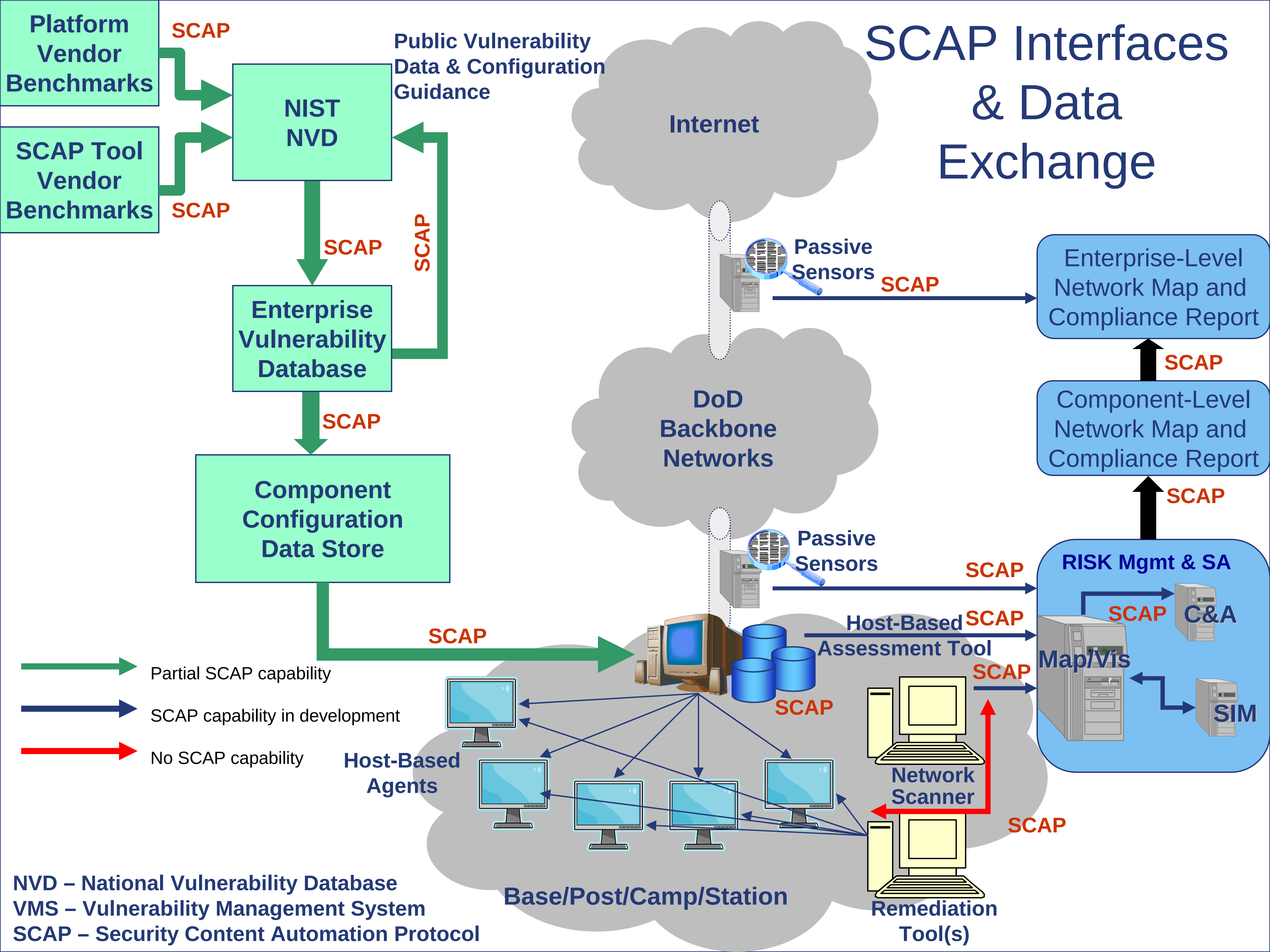


Appropriate details/ summaries shared with CNDSPs and C2 chain

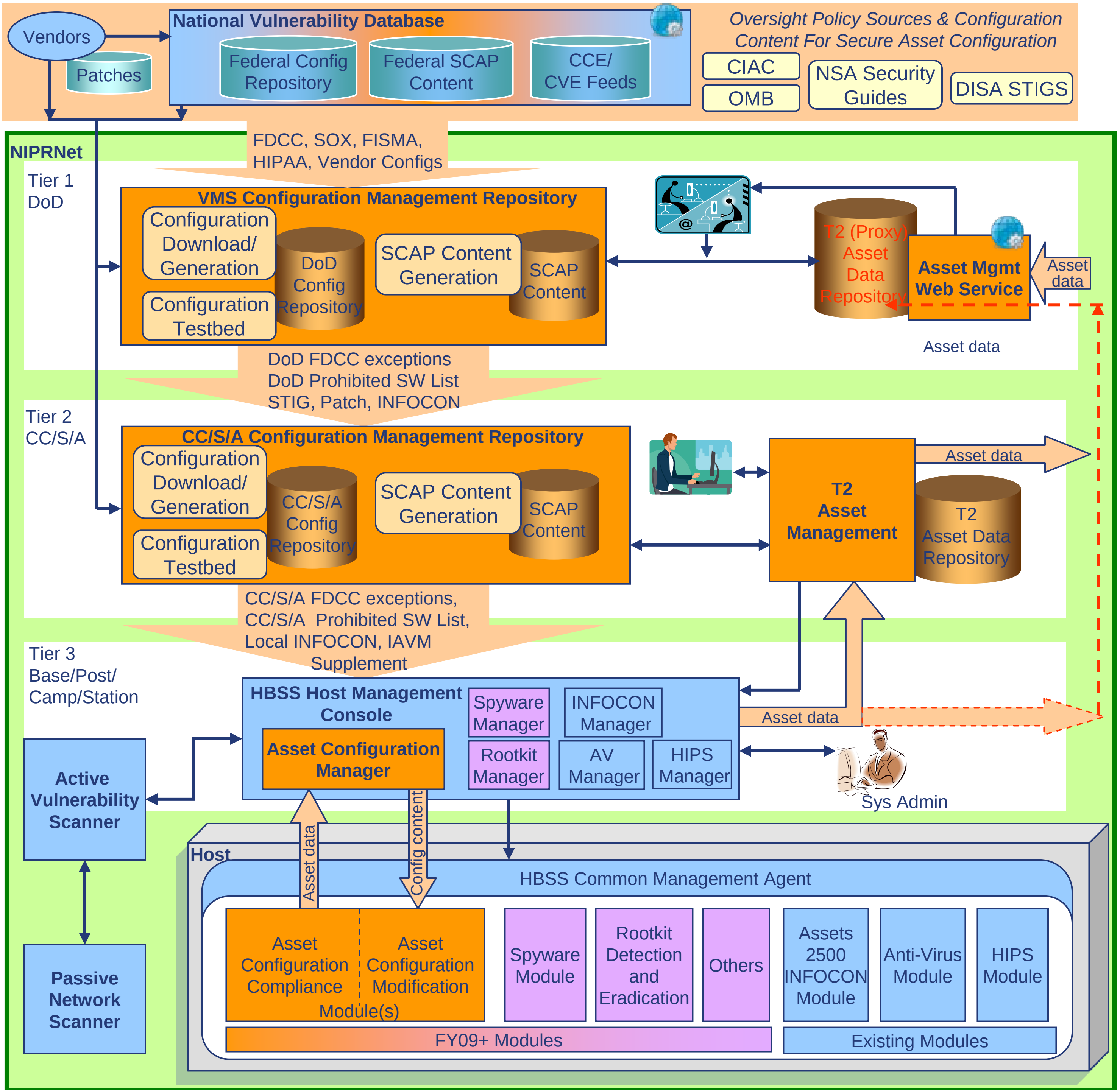
Logical and physical context for alerts

Risk managed against a machine-checkable baseline

SCAP Interfaces & Data Exchange


Platform Vendor Benchmarks
SCAP
SCAP Tool Vendor Benchmarks
SCAP
NIST NVD
Public Vulnerability Data & Configuration Guidance
Internet
SCAP
SCAP
Enterprise Vulnerability Database
SCAP
Component Configuration Data Store
SCAP
Passive Sensors
SCAP
Enterprise-Level Network Map and Compliance Report
SCAP
DoD Backbone Networks
Component-Level Network Map and Compliance Report
SCAP
Passive Sensors
SCAP
RISK Mgmt & SA
SCAP
C&A
Host-Based Assessment Tool
SCAP
Map/Vis
SCAP
SIM
SCAP
Network Scanner
SCAP
Host-Based Agents
Remediation Tool(s)
Base/Post/Camp/Station
Partial SCAP capability
SCAP capability in development
No SCAP capability

NVD – National Vulnerability Database
VMS – Vulnerability Management System
SCAP – Security Content Automation Protocol



Vendors

Patches

National Vulnerability Database

Federal Config Repository

Federal SCAP Content

CCE/ CVE Feeds

Oversight Policy Sources & Configuration Content For Secure Asset Configuration

CIAC

OMB

NSA Security Guides

DISA STIGS

FDCC, SOX, FISMA, HIPAA, Vendor Configs

NIPRNet

Tier 1 DoD

VMS Configuration Management Repository

Configuration Download/ Generation

Configuration Testbed

DoD Config Repository

SCAP Content Generation

SCAP Content

T2 (Proxy) Asset Data Repository

Asset Mgmt Web Service

Asset data

Asset data

DoD FDCC exceptions
DoD Prohibited SW List
STIG, Patch, INFOCON

Tier 2 CC/S/A

CC/S/A Configuration Management Repository

Configuration Download/ Generation

Configuration Testbed

CC/S/A Config Repository

SCAP Content Generation

SCAP Content

T2 Asset Management

Asset data

T2 Asset Data Repository

CC/S/A FDCC exceptions,
CC/S/A Prohibited SW List,
Local INFOCON, IAVM Supplement

Tier 3 Base/Post/ Camp/Station

HBSS Host Management Console

Asset Configuration Manager

Spyware Manager

INFOCON Manager

Rootkit Manager

AV Manager

HIPS Manager

Asset data

Sys Admin

Active Vulnerability Scanner

Passive Network Scanner

Host

Asset data

Config content

HBSS Common Management Agent

Asset Configuration Compliance

Asset Configuration Modification

Module(s)

Spyware Module

Rootkit Detection and Eradication

Others

Assets 2500 INFOCON Module

Anti-Virus Module

HIPS Module

FY09+ Modules

Existing Modules

Enhanced Configuration Management and Computer Network Defense

🟧	CM Capability
🟪	CND Capability To Be Developed Under Other initiatives
🟦	Existing Capability

Unclassified

Questions

- **Contact Information**

Dan Schmidt
Ph. 410-854-3889
Email: dschm2@nsa.gov