CVE and CVSS

Steve Christey
Principal Infosec Engineer
The MITRE Corporation

September 27, 2010

Who Am I?

- ❑Editor of the CVE List
- ❑Contributor to CVSS SIG
- ❑Popularized “responsible disclosure”
- ❑16 years’ Experience
- ❑MITRE: not-for-profit organization, operating four FFRDC’s (DHS, FAA, IRS/VA, DoD)

As a public interest company, MITRE works in partnership with the government applying systems engineering and advanced technology to address issues of critical national importance.

The Problem Area

- ❑What vulnerabilities might exist in software that has been deployed on my networks?
- ❑How do I find the necessary details?
- ❑How do I prioritize what to fix?
- ❑How do I do this in a vendor-independent way?

Part of the Solution: Standardized Identifiers and Severity Ratings

- **CVE – Common Vulnerabilities and Exposures**
  - A standard way to identify a vulnerability with standard naming convention
  - http://cve.mitre.org
- **CVSS – Common Vulnerability Scoring System**
  - A standard way to measure vulnerability severity rating
  - http://www.first.org/cvss/

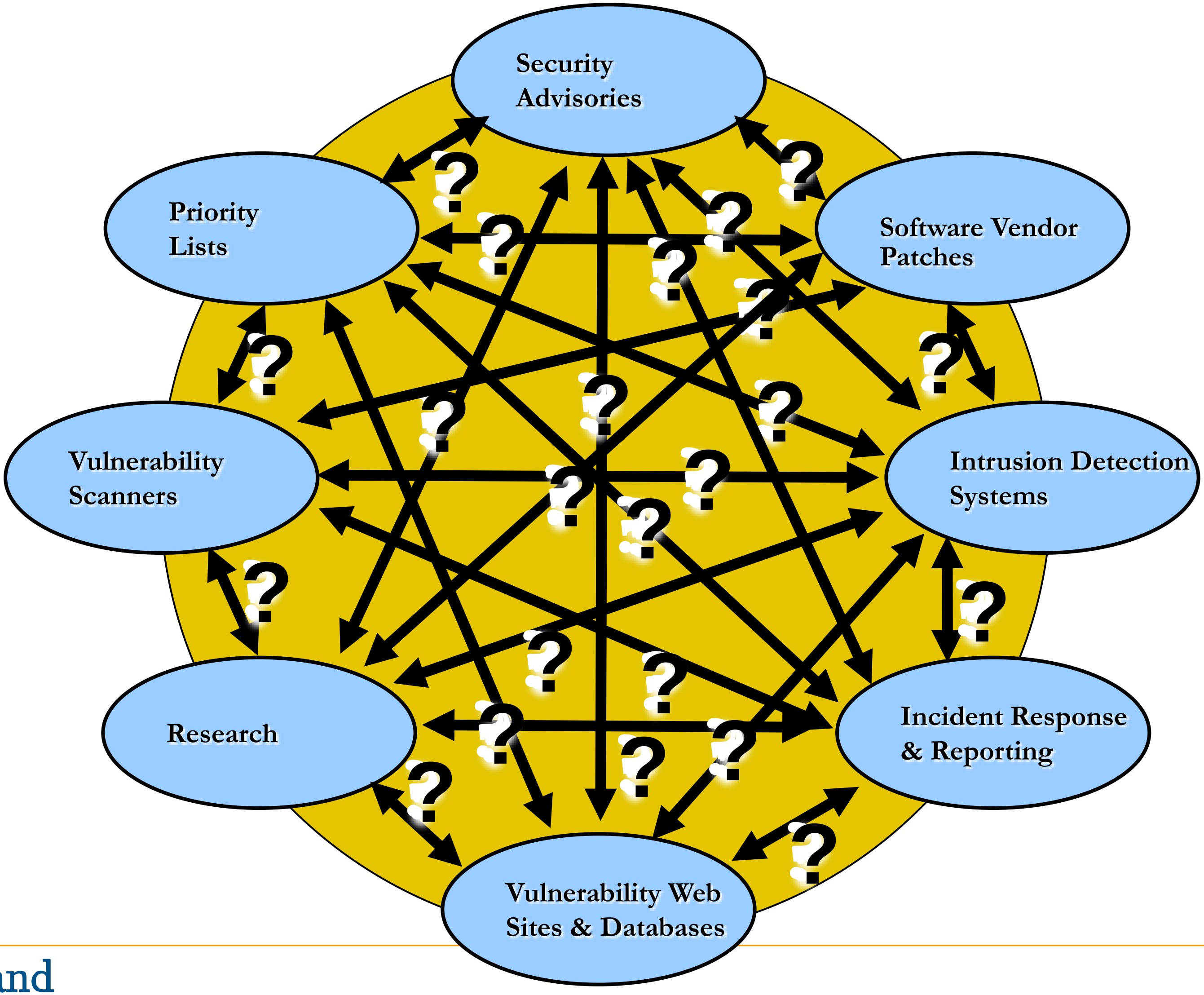
More standards and related information can be found at: http://makingsecuritymeasurable.mitre.org/

International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

Why CVE?

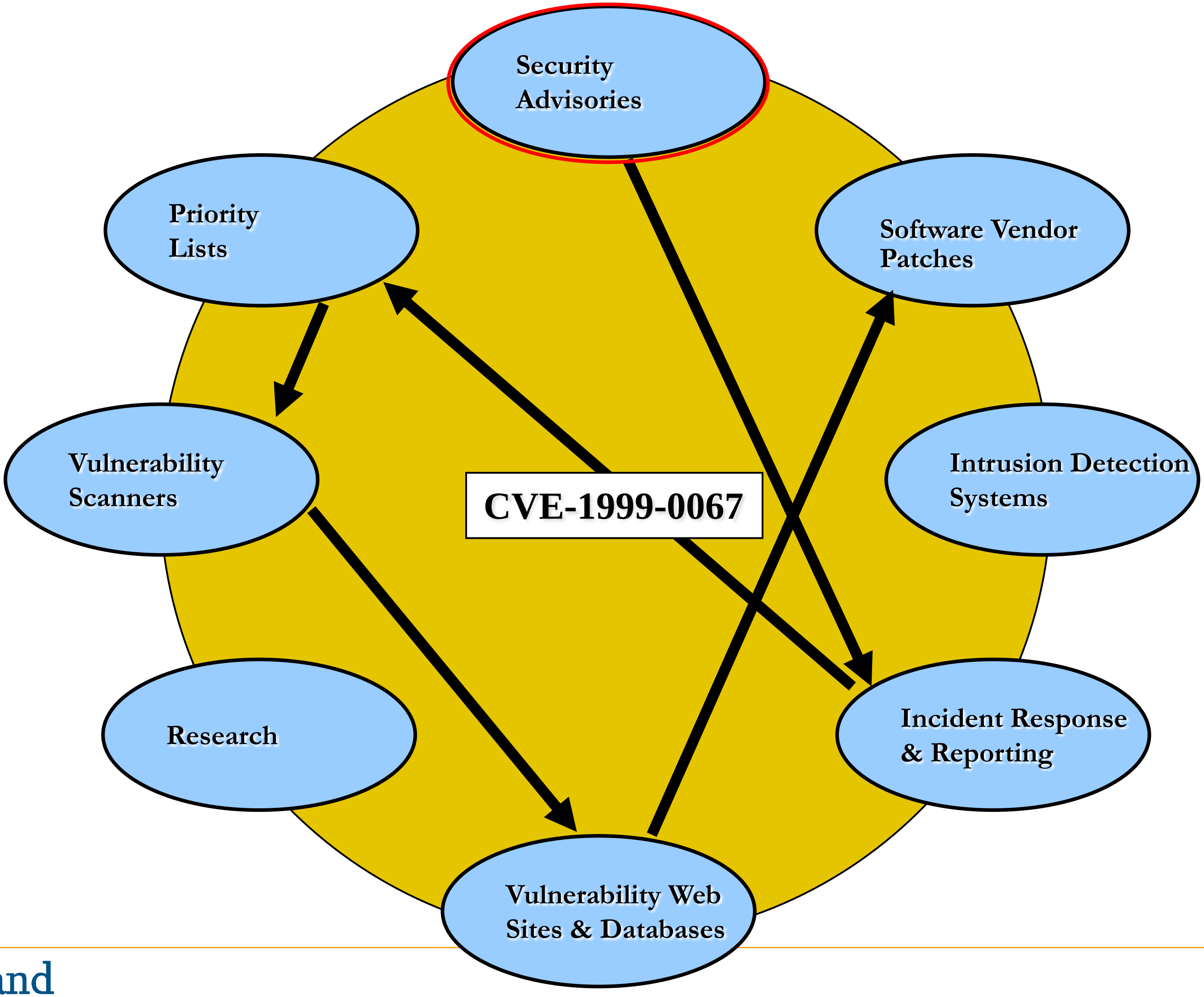
- ❑ **Integrating CVE into your vulnerability management process allows for:**
  - – Speaking the same language. A single name for a single vulnerability located in your environment.
  - – Information sharing between multiple systems / platforms.
  - – The same vulnerability, identified by different vendors, will always have the same CVE.
  - – Consolidation of different sources of vulnerability data that use CVE

Difficult to Integrate Information on Vulnerabilities and Exposures

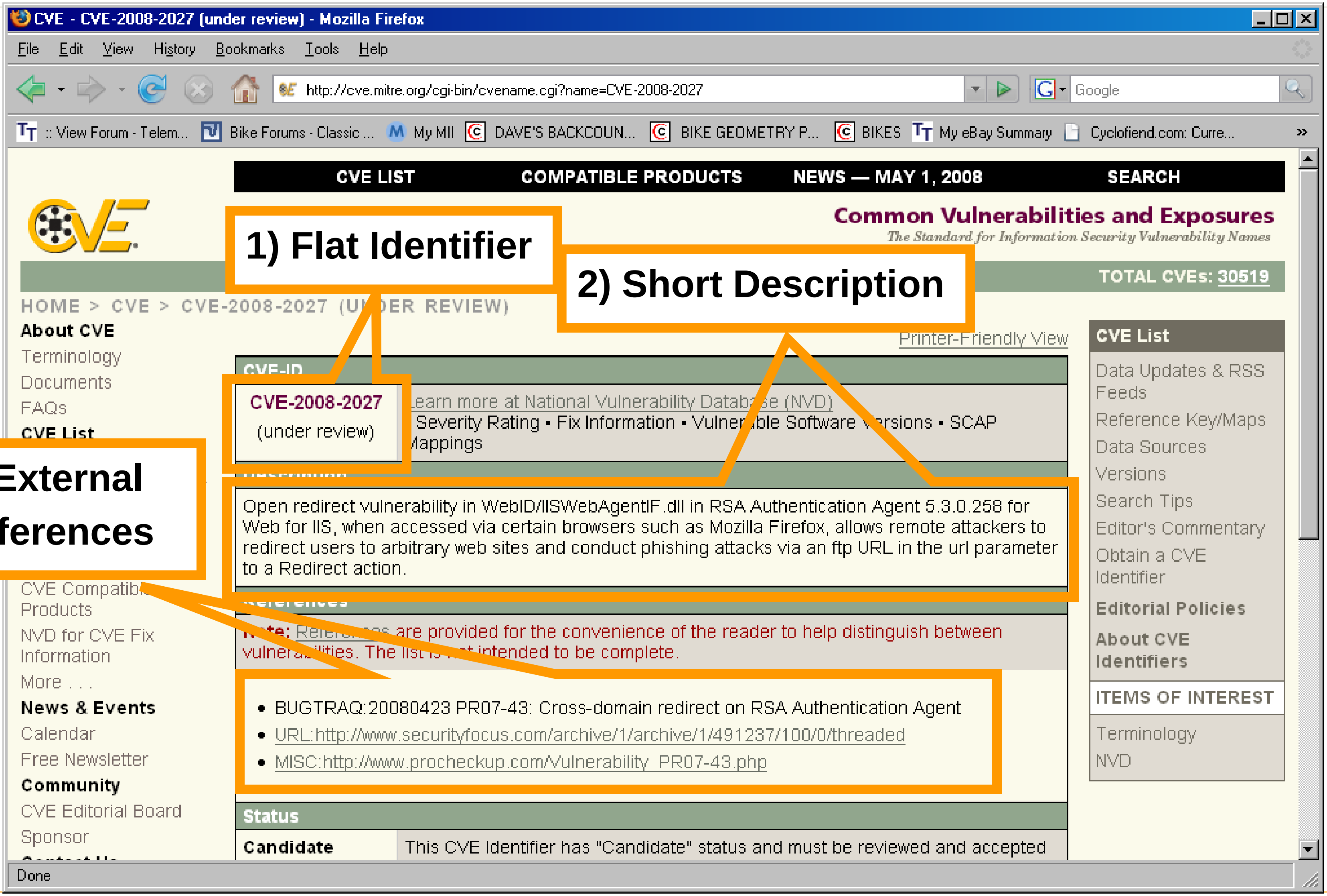

Security Advisories
Priority Lists
Software Vendor Patches
Vulnerability Scanners
Intrusion Detection Systems
Research
Incident Response & Reporting
Vulnerability Web Sites & Databases
?

The HS SEDI FFRDC is managed and operated by The MITRE Corporation for DHS.

The CVE List provides a path for integrating information on Vulnerabilities and Exposures



CVE Entries: Dictionary, not a Database



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

TOTAL CVEs: 30519

HOME > CVE > CVE-2008-2027 (UNDER REVIEW)

CVE-ID

CVE-2008-2027 (under review)

Learn more at National Vulnerability Database (NVD)
Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Open redirect vulnerability in WebID/IISWebAgentIF.dll in RSA Authentication Agent 5.3.0.258 for Web for IIS, when accessed via certain browsers such as Mozilla Firefox, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via an ftp URL in the url parameter to a Redirect action.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20080423 PR07-43: Cross-domain redirect on RSA Authentication Agent
- URL:http://www.securityfocus.com/archive/1/archive/1/491237/100/0/threaded
- MISC:http://www.procheckup.com/Vulnerability_PR07-43.php

Status

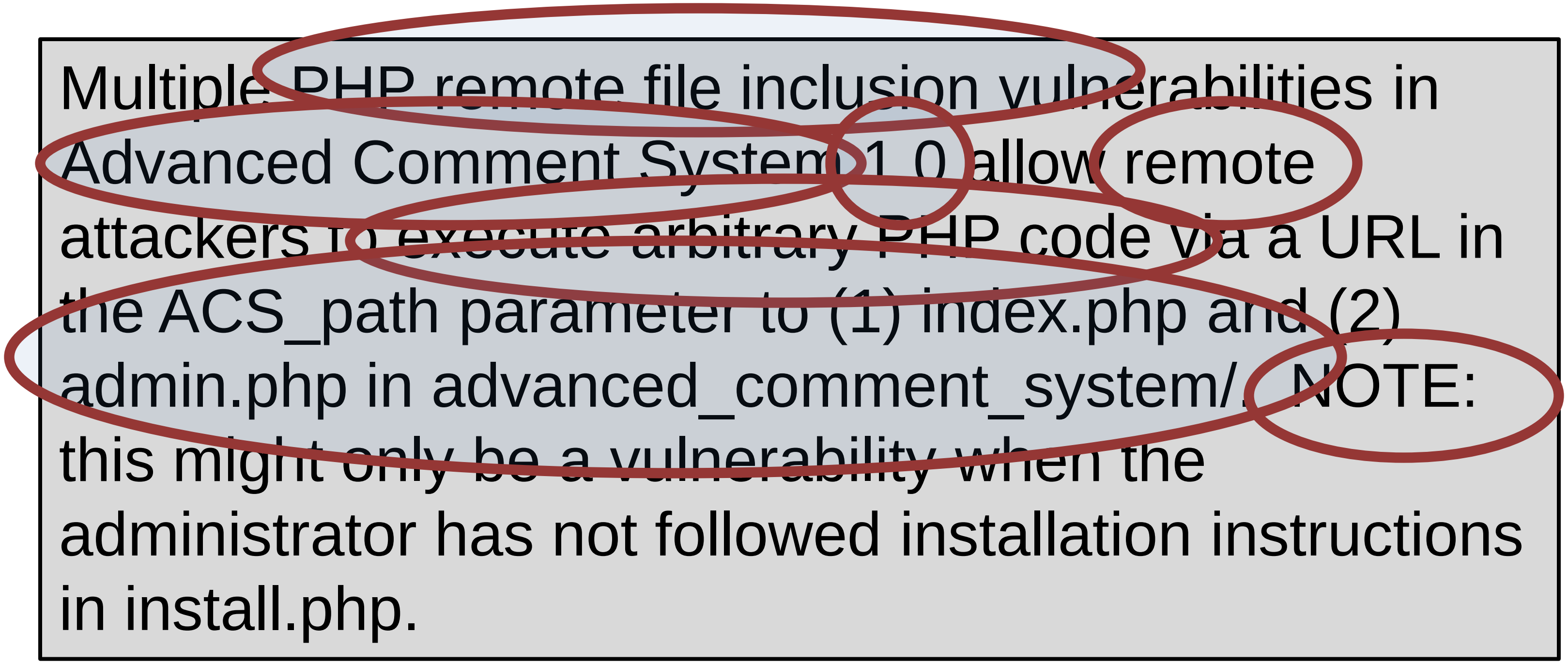
Candidate — This CVE Identifier has "Candidate" status and must be reviewed and accepted

1) Flat Identifier

2) Short Description

3) External References

Anatomy of a CVE Description: CVE-2009-4623

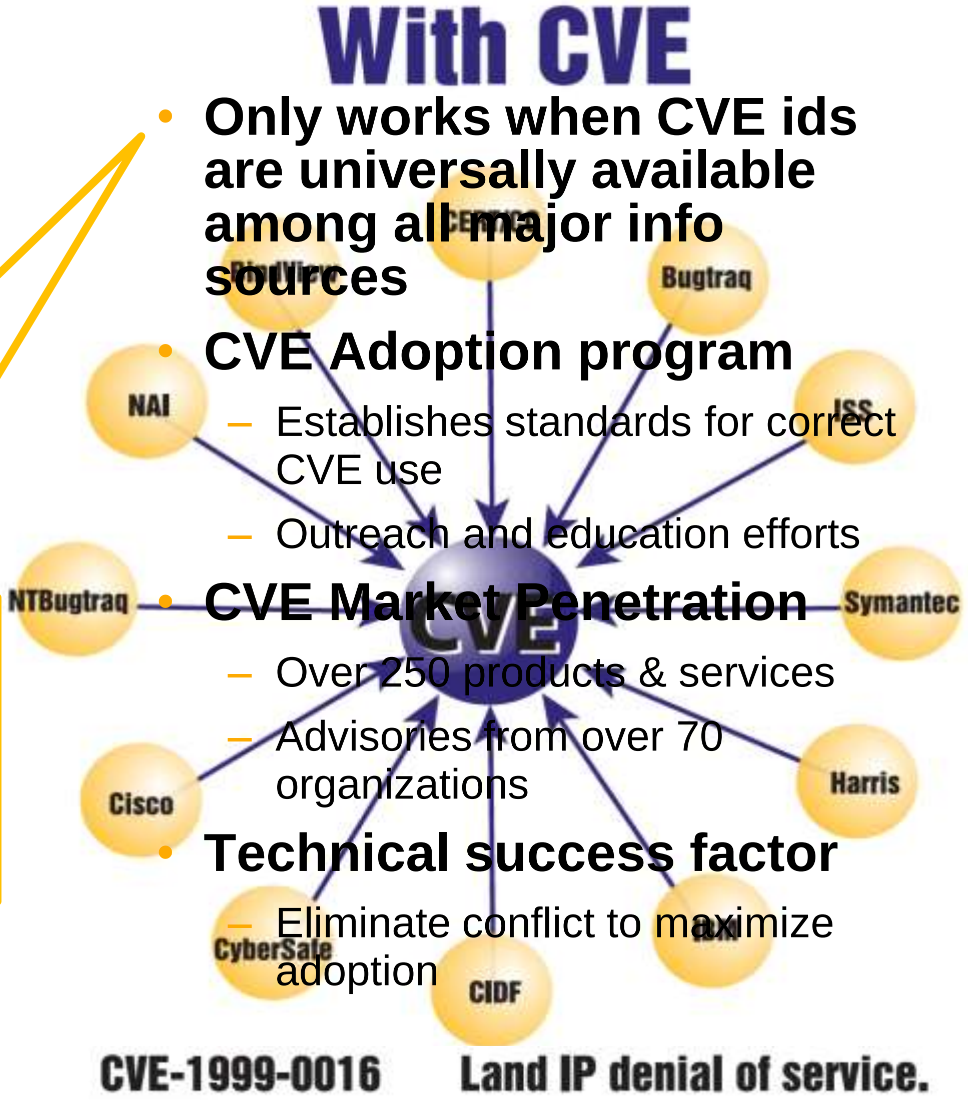


Multiple PHP remote file inclusion vulnerabilities in Advanced Comment System 1.0 allow remote attackers to execute arbitrary PHP code via a URL in the ACS_path parameter to (1) index.php and (2) admin.php in advanced_comment_system/. NOTE: this might only be a vulnerability when the administrator has not followed installation instructions in install.php.

Flaw type, vendor name, product name, affected versions, remote/local, impact, attack vectors, clarifiers.

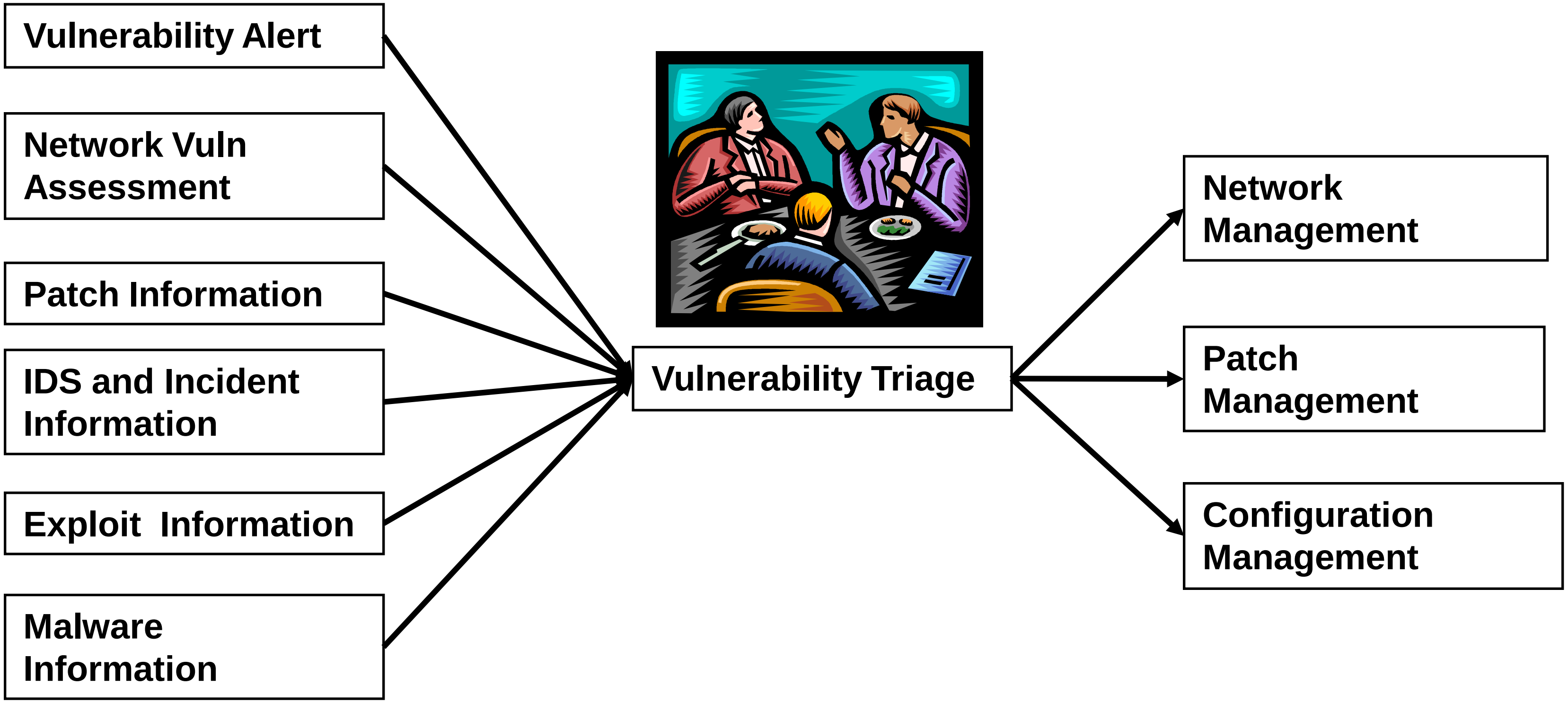
Value: Primary User – Vulnerability Triage

- **Goal: Respond to new vulnerabilities**
  - Patch, reconfigure, block, stop service
- **Collaboration**
  - Security ops, system designers, network architects, financial risk mgmt
- **Considers multiple sources**
  - Vulnerability alert services, vulnerability scanners, IDS alerts, security advisories, patch information
- **MAJOR ROADBLOCK**
  - Which sources are talking about the same vulnerability?



- **Only works when CVE ids are universally available among all major info sources**
- **CVE Adoption program**
  - Establishes standards for correct CVE use
  - Outreach and education efforts
- **CVE Market Penetration**
  - Over 250 products & services
  - Advisories from over 70 organizations
- **Technical success factor**
  - Eliminate conflict to maximize adoption

How CVEs Are Used



Vulnerability Alert

Network Vuln Assessment

Patch Information

IDS and Incident Information

Exploit Information

Malware Information

Vulnerability Triage

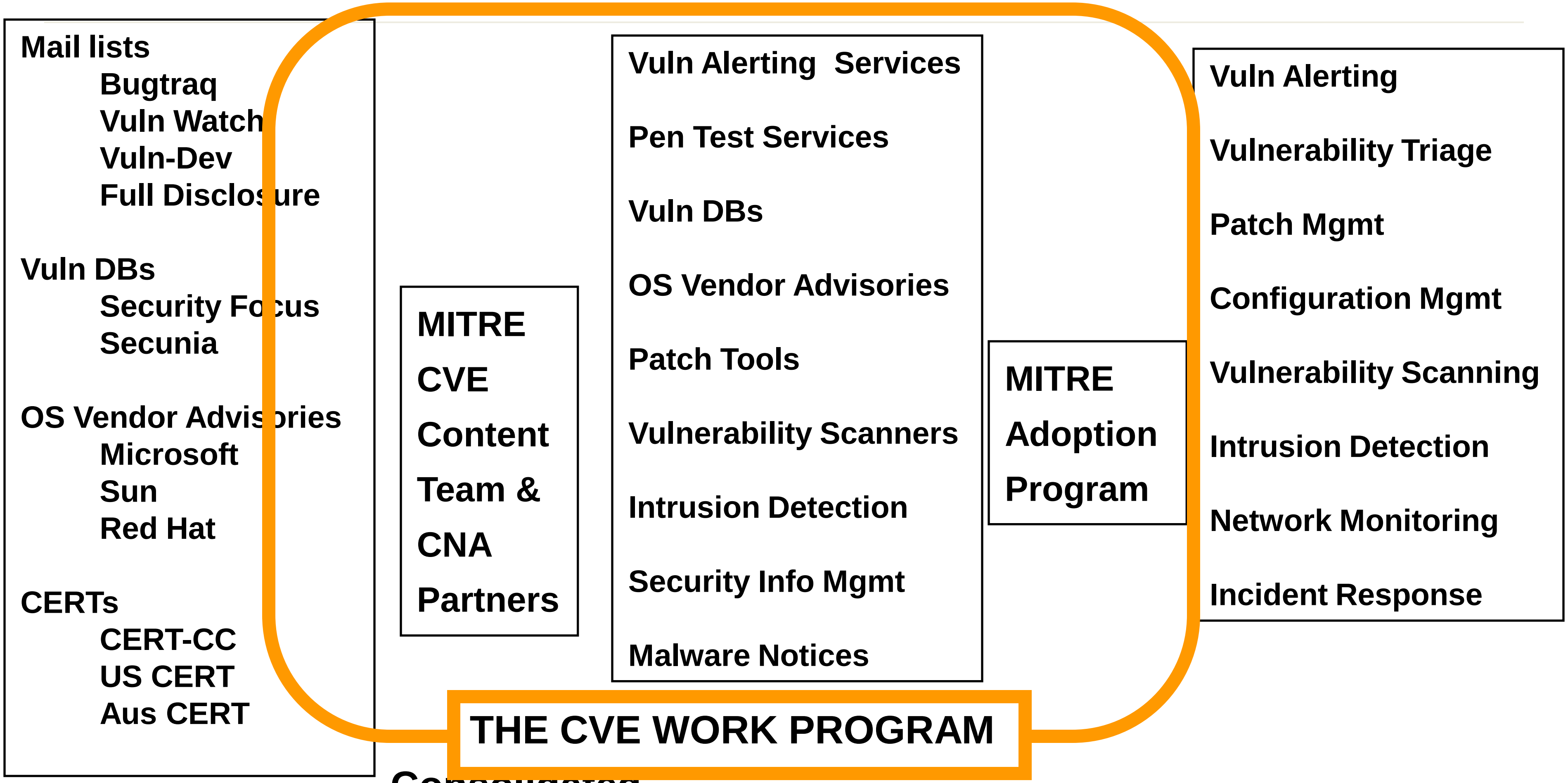
Network Management

Patch Management

Configuration Management

- **Used to correlate vulnerability information**
  - Like VINs at the Registry of Motor Vehicles
- **Slashes analysis time**
  - Users estimate by a factor of 10, at least

How CVE’s Are Produced



Mail lists
- Bugtraq
- Vuln Watch
- Vuln-Dev
- Full Disclosure

Vuln DBs
- Security Focus
- Secunia

OS Vendor Advisories
- Microsoft
- Sun
- Red Hat

CERTs
- CERT-CC
- US CERT
- Aus CERT

MITRE CVE Content Team & CNA Partners

Vuln Alerting Services

Pen Test Services

Vuln DBs

OS Vendor Advisories

Patch Tools

Vulnerability Scanners

Intrusion Detection

Security Info Mgmt

Malware Notices

MITRE Adoption Program

Vuln Alerting

Vulnerability Triage

Patch Mgmt

Configuration Mgmt

Vulnerability Scanning

Intrusion Detection

Network Monitoring

Incident Response

THE CVE WORK PROGRAM

New Disclosures

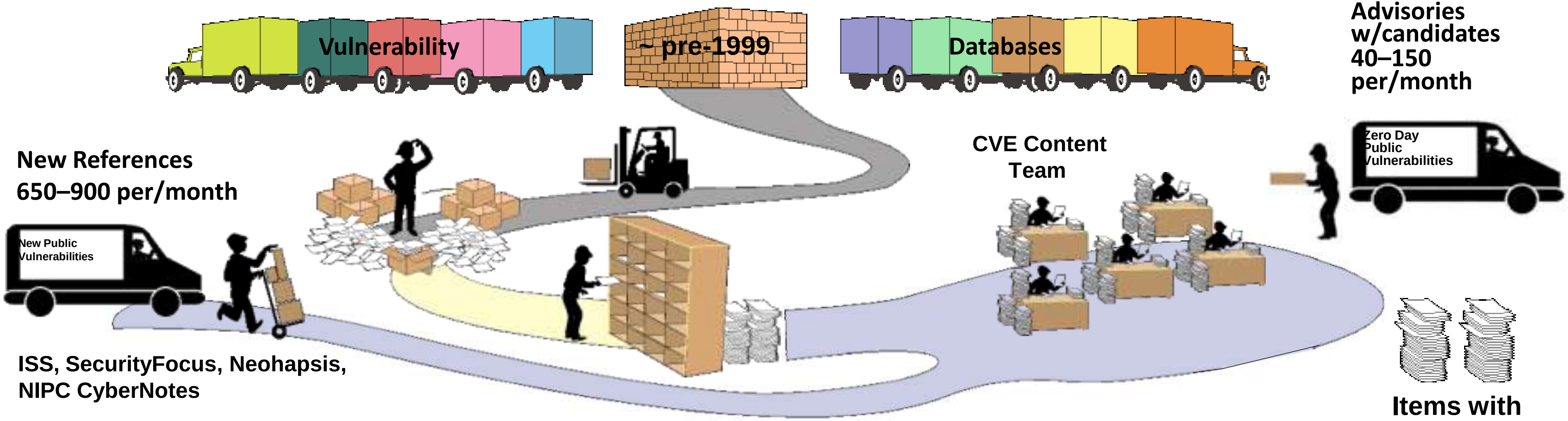
Consolidated into CVEs & Published

CVE IDs Put Into Products by Vendors

Product Self-Cert

Enterprise Vulnerability Management

Where the CVE Items Come From



Legacy Submissions

AXENT, BindView, Harris, Cisco, CERIAS

Hiverworld, SecurityFocus, ISS, NAI, Symantec, Nessus

Alerts & Advisories w/candidates 40–150 per/month

New References 650–900 per/month

CVE Content Team

ISS, SecurityFocus, Neohapsis, NIPC CyberNotes

Items with Unique CVE Names

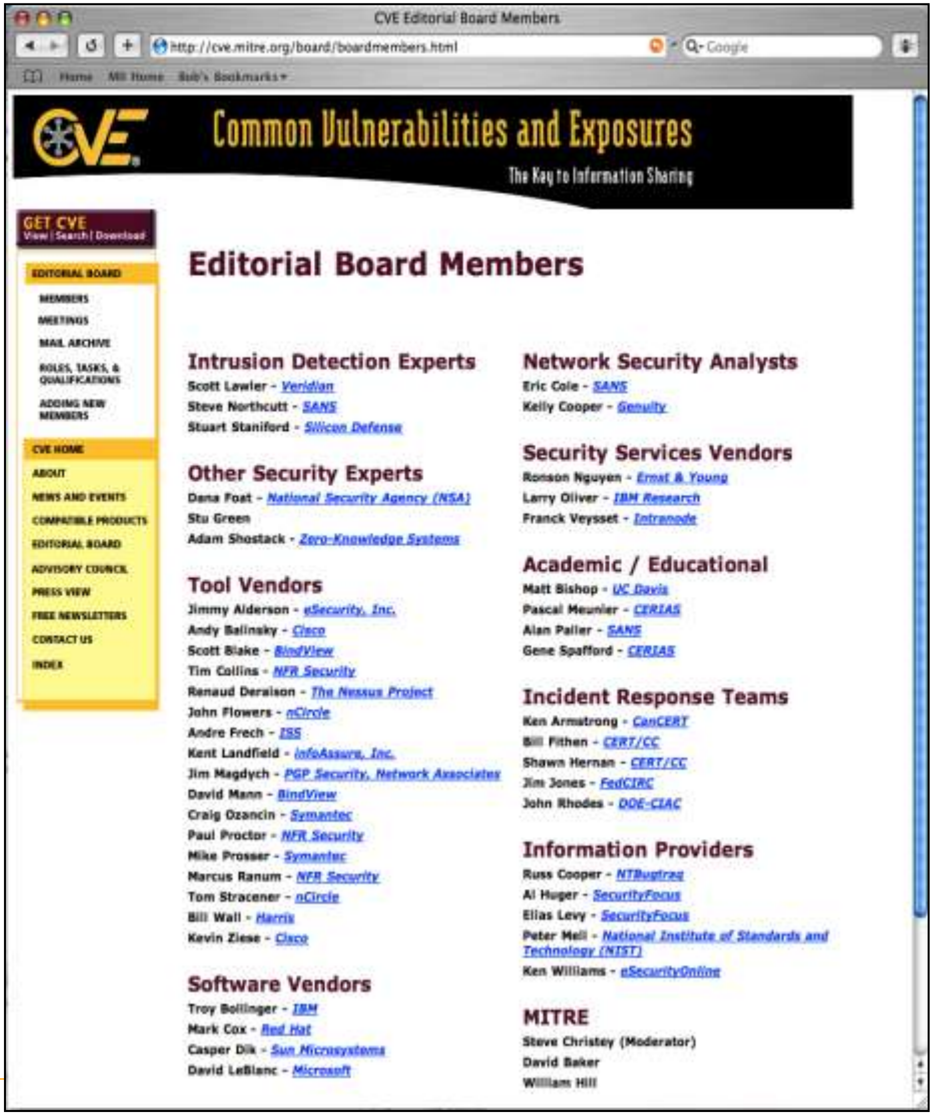
~40,976

CVE Editorial Board

BIND VIEW · NFR SECURITY · MITRE · Sun · CITADEL SECURITY SOFTWARE · IBM · NIST National Institute of Standards and Technology · STAT · Carnegie Mellon Software Engineering Institute · CERIAS · SANS INSTITUTE · INTERNET SECURITY SYSTEMS · Microsoft · redhat · U.S. Department of Energy CIAC · ca Computer Associates · security-focus.com · GENERAL DYNAMICS Advanced Information Systems · SILICON DEFENSE · GUARDEDNET · symantec · Nessus · EWA · nCircle NETWORK SECURITY · CISCO SYSTEMS · INTRANODE · UCDAVIS

CVE Editorial Board

- Includes mostly technical representatives from 35 different organizations including researchers, tool vendors, response teams, and end users
- Reviews and approves CVE entries
- Discusses issues related to CVE maintenance
- Holds monthly meetings (face-to-face or phone)
- Maintains publicly viewable mailing list archives [cve.mitre.org/board/archives]



Editorial Board Members

Intrusion Detection Experts

Scott Lawler - Veridian
Steve Northcutt - SANS
Stuart Staniford - Silicon Defense

Other Security Experts

Dana Foat - National Security Agency (NSA)
Stu Green
Adam Shostack - Zero-Knowledge Systems

Tool Vendors

Jimmy Alderson - eSecurity, Inc.
Andy Balinsky - Cisco
Scott Blake - BindView
Tim Collins - NFR Security
Renaud Deraison - The Nessus Project
John Flowers - nCircle
Andre Frech - ISS
Kent Landfield - infoAssure, Inc.
Jim Magdych - PGP Security, Network Associates
David Mann - BindView
Craig Ozancin - Symantec
Paul Proctor - NFR Security
Mike Prosser - Symantec
Marcus Ranum - NFR Security
Tom Stracener - nCircle
Bill Wall - Harris
Kevin Ziese - Cisco

Software Vendors

Troy Bollinger - IBM
Mark Cox - Red Hat
Casper Dik - Sun Microsystems
David LeBlanc - Microsoft

Network Security Analysts

Eric Cole - SANS
Kelly Cooper - Genuity

Security Services Vendors

Ronson Nguyen - Ernst & Young
Larry Oliver - IBM Research
Franck Veysset - Intranode

Academic / Educational

Matt Bishop - UC Davis
Pascal Meunier - CERIAS
Alan Paller - SANS
Gene Spafford - CERIAS

Incident Response Teams

Ken Armstrong - CanCERT
Bill Fithen - CERT/CC
Shawn Hernan - CERT/CC
Jim Jones - FedCIRC
John Rhodes - DOE-CIAC

Information Providers

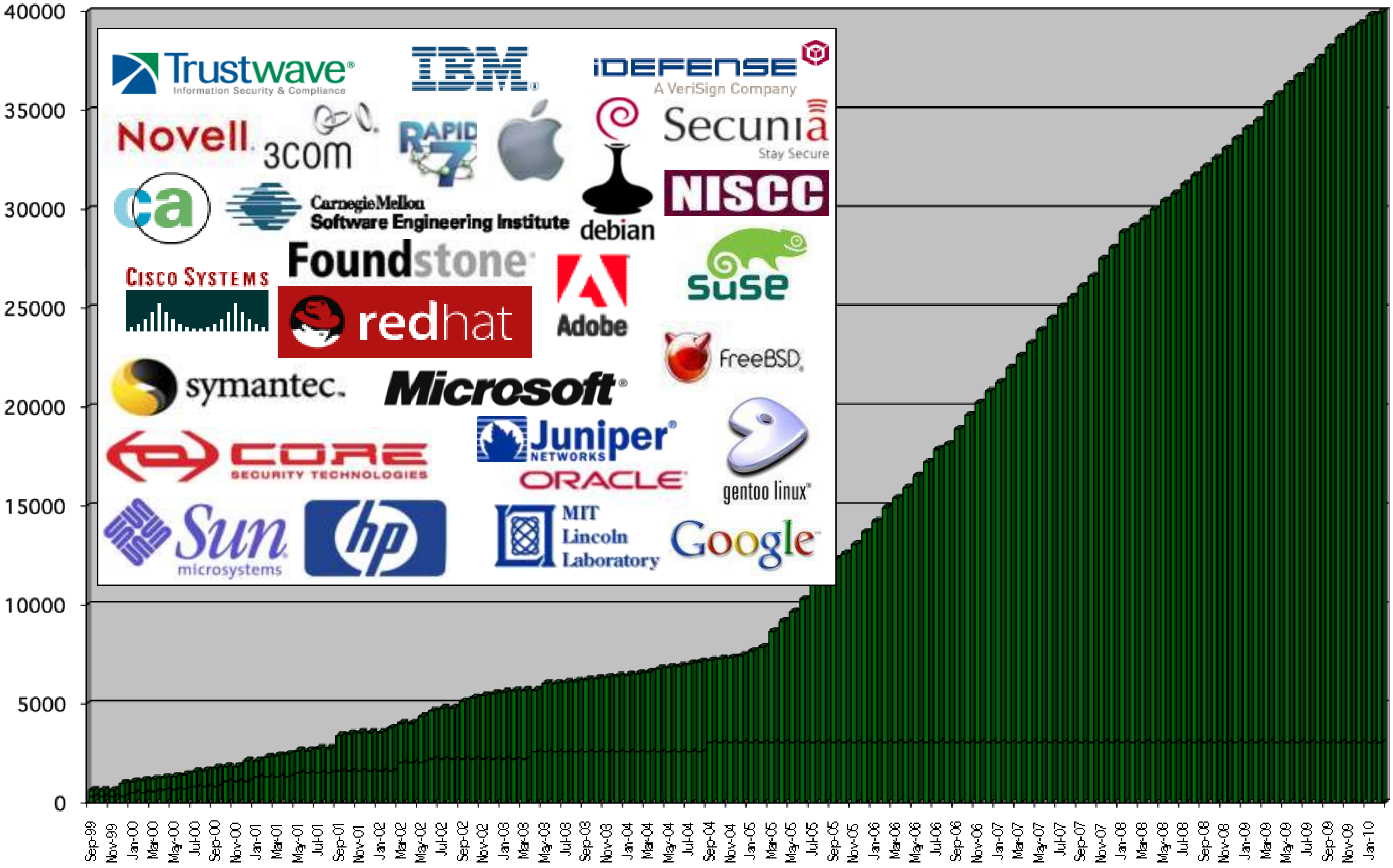
Russ Cooper - NTBugtraq
Al Huger - SecurityFocus
Elias Levy - SecurityFocus
Peter Mell - National Institute of Standards and Technology (NIST)
Ken Williams - eSecurityOnline

MITRE

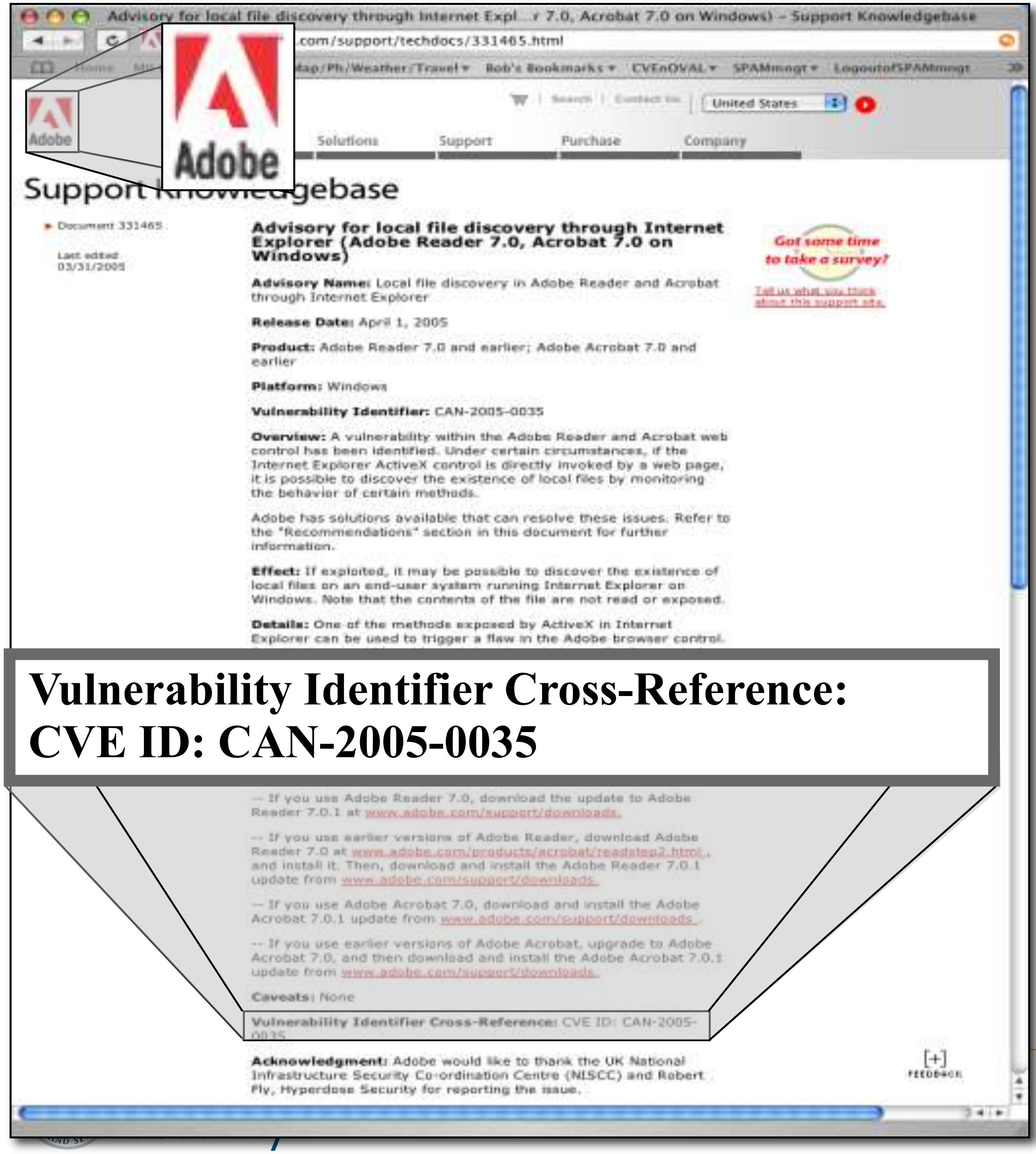
Steve Christey (Moderator)
David Baker
William Hill

[cve.mitre.org/board/boardmembers.html]

CVE 1999 to 2010



Many organizations are reserving CVE names and using them in their alerts and advisories



Advisory for local file discovery through Internet Expl…r 7.0, Acrobat 7.0 on Windows) – Support Knowledgebase
.com/support/techdocs/331465.html
Map/Ph/Weather/Travel ▾
Bob's Bookmarks ▾
CVEnOVAL ▾
SPAMmngt ▾
LogoutofSPAMmngt
Search
Contact Us
United States
Solutions
Support
Purchase
Company
Adobe
Got some time to take a survey?
Tell us what you think about this support site.
[+] FEEDBACK

Support Knowledgebase

Document 331465

Last edited 03/31/2005

Advisory for local file discovery through Internet Explorer (Adobe Reader 7.0, Acrobat 7.0 on Windows)

Advisory Name: Local file discovery in Adobe Reader and Acrobat through Internet Explorer

Release Date: April 1, 2005

Product: Adobe Reader 7.0 and earlier; Adobe Acrobat 7.0 and earlier

Platform: Windows

Vulnerability Identifier: CAN-2005-0035

Overview: A vulnerability within the Adobe Reader and Acrobat web control has been identified. Under certain circumstances, if the Internet Explorer ActiveX control is directly invoked by a web page, it is possible to discover the existence of local files by monitoring the behavior of certain methods.

Adobe has solutions available that can resolve these issues. Refer to the "Recommendations" section in this document for further information.

Effect: If exploited, it may be possible to discover the existence of local files on an end-user system running Internet Explorer on Windows. Note that the contents of the file are not read or exposed.

Details: One of the methods exposed by ActiveX in Internet Explorer can be used to trigger a flaw in the Adobe browser control.

-- If you use Adobe Reader 7.0, download the update to Adobe Reader 7.0.1 at www.adobe.com/support/downloads.

-- If you use earlier versions of Adobe Reader, download Adobe Reader 7.0 at www.adobe.com/products/acrobat/readstep2.html , and install it. Then, download and install the Adobe Reader 7.0.1 update from www.adobe.com/support/downloads.

-- If you use Adobe Acrobat 7.0, download and install the Adobe Acrobat 7.0.1 update from www.adobe.com/support/downloads .

-- If you use earlier versions of Adobe Acrobat, upgrade to Adobe Acrobat 7.0, and then download and install the Adobe Acrobat 7.0.1 update from www.adobe.com/support/downloads.

Caveats: None

Vulnerability Identifier Cross-Reference: CVE ID: CAN-2005-0035

Acknowledgment: Adobe would like to thank the UK National Infrastructure Security Co-ordination Centre (NISCC) and Robert Fly, Hyperdose Security for reporting the issue.

Vulnerability Identifier Cross-Reference:
CVE ID: CAN-2005-0035

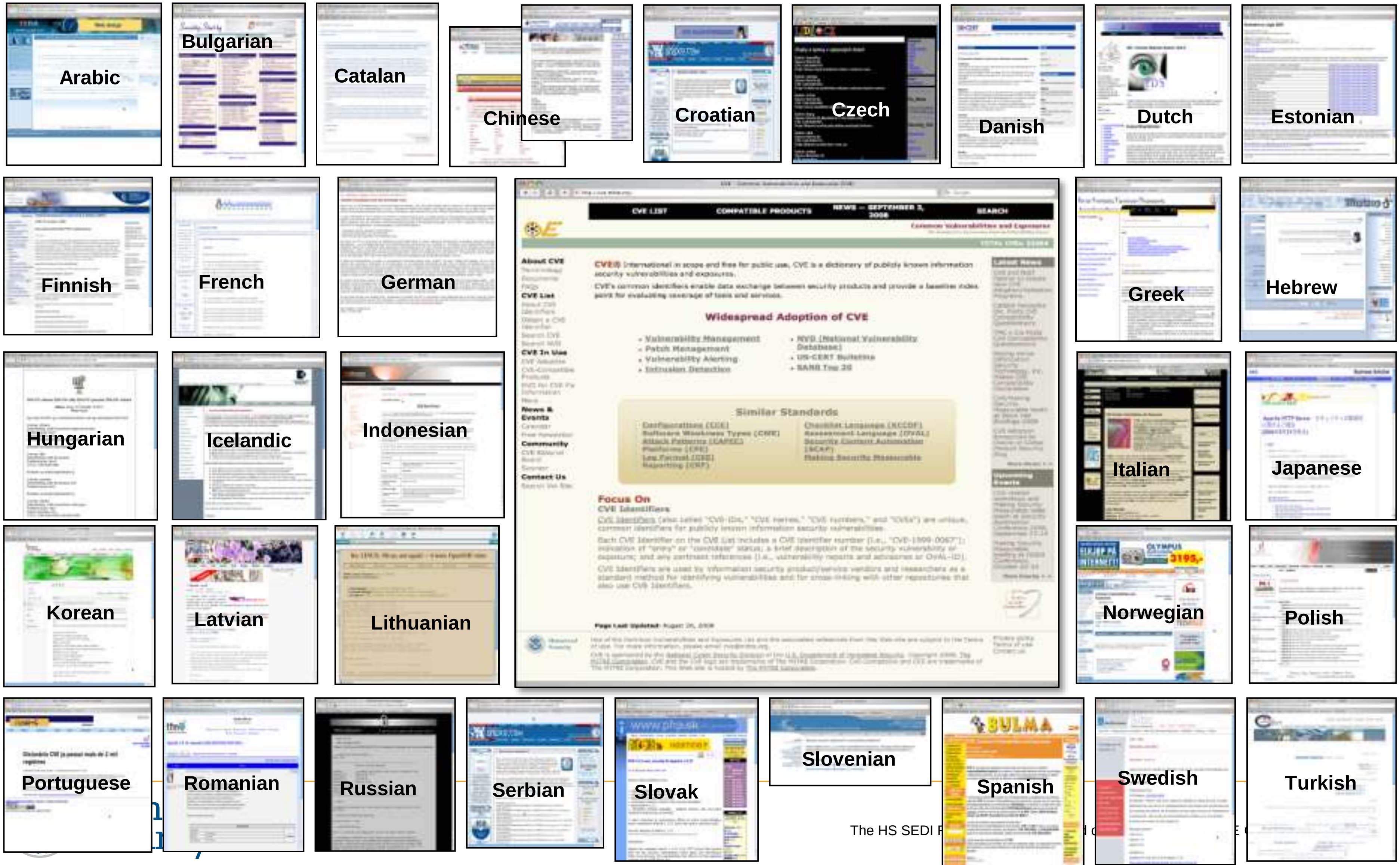
To-date, CVE names have been included in thousands of advisories from:

- ISS X-Force
- Rain Forest Puppy
- BindView
- CERT/CC
- COMPAQ
- Ernst & Young
- NSFOCUS
- VIGILANTe.com
- SecurityFocus
- Caldera
- EnGarde Secure Linux
- Mandrake Linux
- Foundstone
- iDEFENSE
- Symantec
- Beyond Security Ltd
- Digital Defense Inc.
- The OpenPKG Project
- The FreeBSD Project
- The NetBSD Project
- Slackware Linux
- Conectiva Linux
- AusCERT
- ThaiCERT
- HKCERT
- SURFnet-CERT
- Pine Digital Security
- Slovenian CERT
- FedoraNEWS.ORG
- CASESContact.org
- C.Enter Information-Technology
- Critical Watch
- CASESContact.org
- Ubuntu Linux
- AVET Info & Network Security
- Oracle
- IBM
- @stake
- NAI
- SGI
- Microsoft
- eEye
- CISCO
- Rapid 7
- Sanctum
- Corsaire
- Red Hat
- Cert-IST
- Alcatel
- Debian
- Apple
- HP
- DHS/NIPC
- KDE e. V.
- Core-ST
- Gentoo Linux
- Immunix
- e-Matters
- Sun
- French CERT
- CERTin
- OpenSSL
- CERT Polska
- NoMachine
- K-OTik Security
- TurboLinux
- Zone-H.org
- K-OTik Security
- NISCC
- ACROS Security
- Adobe

http://www.adobe.com/support/techdocs/331465.htm

CVE is Widely Used & Available …… 43,335 and climbing…

HS SEDI
Homeland Security Systems Engineering and Development Institute



CVE LIST | COMPATIBLE PRODUCTS | NEWS — SEPTEMBER 3, 2008 | SEARCH

Common Vulnerabilities and Exposures

About CVE
CVE List
CVE In Use
News & Events
Community
Contact Us

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Adoption of CVE

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection
- NVD (National Vulnerability Database)
- US-CERT Bulletins
- SANS Top 20

Similar Standards

Configurations (CCE)
Software Weakness Types (CWE)
Attack Patterns (CAPEC)
Platforms (CPE)
Log Format (CEE)
Reporting (CRF)
Checklist Language (XCCDF)
Assessment Language (OVAL)
Security Content Automation (SCAP)
Making Security Measurable

Focus On
CVE Identifiers

Page Last Updated: August 26, 2008

Conference Outreach Efforts

JULY 23-25, 2003, WASHINGTON CONVENTION CENTER, WASHINGTON, DC
GOVSEC
The Government Security Expo and Conference
all security • all government
AUTHENTICATION CODE REQUIRED

Federal Information Assurance Conference 2003
FIAC
October 21-23, 2003 • The Inn and Conference Center • University of Maryland

LISA '03
OCTOBER 26-31, SAN DIEGO, CA
BY & FOR SYSADMINS!
THE 17TH LARGE INSTALLATION SYSTEMS ADMINISTRATION CONFERENCE

IA Workshop
Feb 2–5, 2004 -- Hyatt Regency Hotel, Atlanta GA
Fighting the Net – Securing Today's Battlefield

THIRTEENTH ANNUAL
RSA Conference 2004
February 23-27 • Moscone Center • San Francisco

MIS TRAINING INSTITUTE
InfoSec World Conference and Expo/2004
March 22 - 24, 2004 Orlando
March 20, 21, 25, 26, 2004 Optional Workshops

MYRTLE BEACH, SOUTH CAROLINA • JUNE 6-9
THE 2004 TECHNO SECURITY CONFERENCE

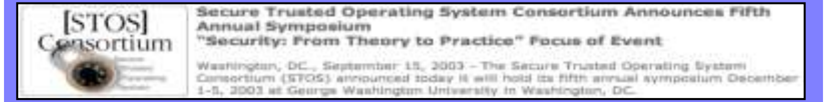
14TH ANNUAL
NetSec 2004
BUILDING THE SECURE ENTERPRISE
ATTEND THE PREMIER CONFERENCE DEVOTED TO NETWORK SECURITY TECHNOLOGY
JUNE 14-16, 2004
SAN FRANCISCO HYATT REGENCY EMBARCADERO

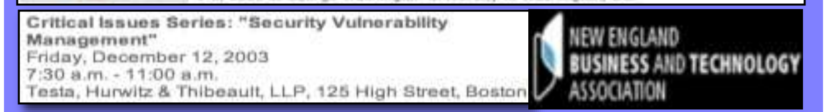
BOOTH

ISSA™
Information Systems Security Association
May Chapter Meeting @ Hewlett-Packard
The New England Chapter

Information Assurance 2003
Building a Cohesive Enterprise Approach
e-gov
Conference: September 15 - 17, 2003
Exhibition: September 17, 2003
Ronald Reagan Building, Washington DC

2003 IEEE International Conference on Systems, Man & Cybernetics
October 5–8, 2003 – Hyatt Regency, Washington, D.C., USA.


[STOS] Consortium
Secure Trusted Operating System Consortium Announces Fifth Annual Symposium
"Security: From Theory to Practice" Focus of Event
Washington, DC., September 15, 2003 – The Secure Trusted Operating System Consortium (STOS) announced today it will hold its fifth annual symposium December 1-5, 2003 at George Washington University in Washington, DC.

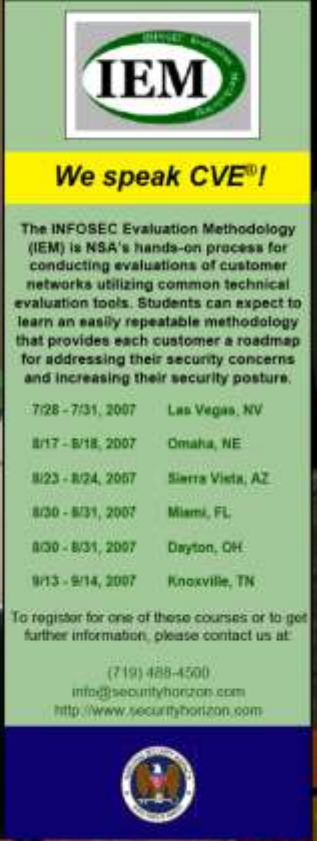

Critical Issues Series: "Security Vulnerability Management"
Friday, December 12, 2003
7:30 a.m. - 11:00 a.m.
Testa, Hurwitz & Thibeault, LLP, 125 High Street, Boston
NEW ENGLAND BUSINESS AND TECHNOLOGY ASSOCIATION

3rd International Conference on COTS-Based Software Systems
1-4 February 2004 Redondo Beach, CA USA
Matching Solutions to Problems
ICCBSS 2004

The British Computer Society Quality Special Interest Group's Annual International SQM and INSPIRE Conferences will be held from Monday 5th to Wednesday 7th of April 2004 at Canterbury Christ Church University College, Kent, UK.
BCS®
The British Computer Society

STC
The Sixteenth Annual Software Technology Conference
19 - 22 April 2004
Salt Palace Convention Center
Salt Lake City, UT

TALK



IEM

We speak CVE®!

The INFOSEC Evaluation Methodology (IEM) is NSA's hands-on process for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture.

7/28 - 7/31, 2007	Las Vegas, NV
8/17 - 8/18, 2007	Omaha, NE
8/23 - 8/24, 2007	Sierra Vista, AZ
8/30 - 8/31, 2007	Miami, FL
8/30 - 8/31, 2007	Dayton, OH
9/13 - 9/14, 2007	Knoxville, TN

To register for one of these courses or to get further information, please contact us at:

(719) 488-4500
info@securityhorizon.com
http://www.securityhorizon.com

Booths

Live Demo

NetIQ

Developer Days 05

Developer Days 06

BigFix

ArcSight

ThreatGuard

McAfee

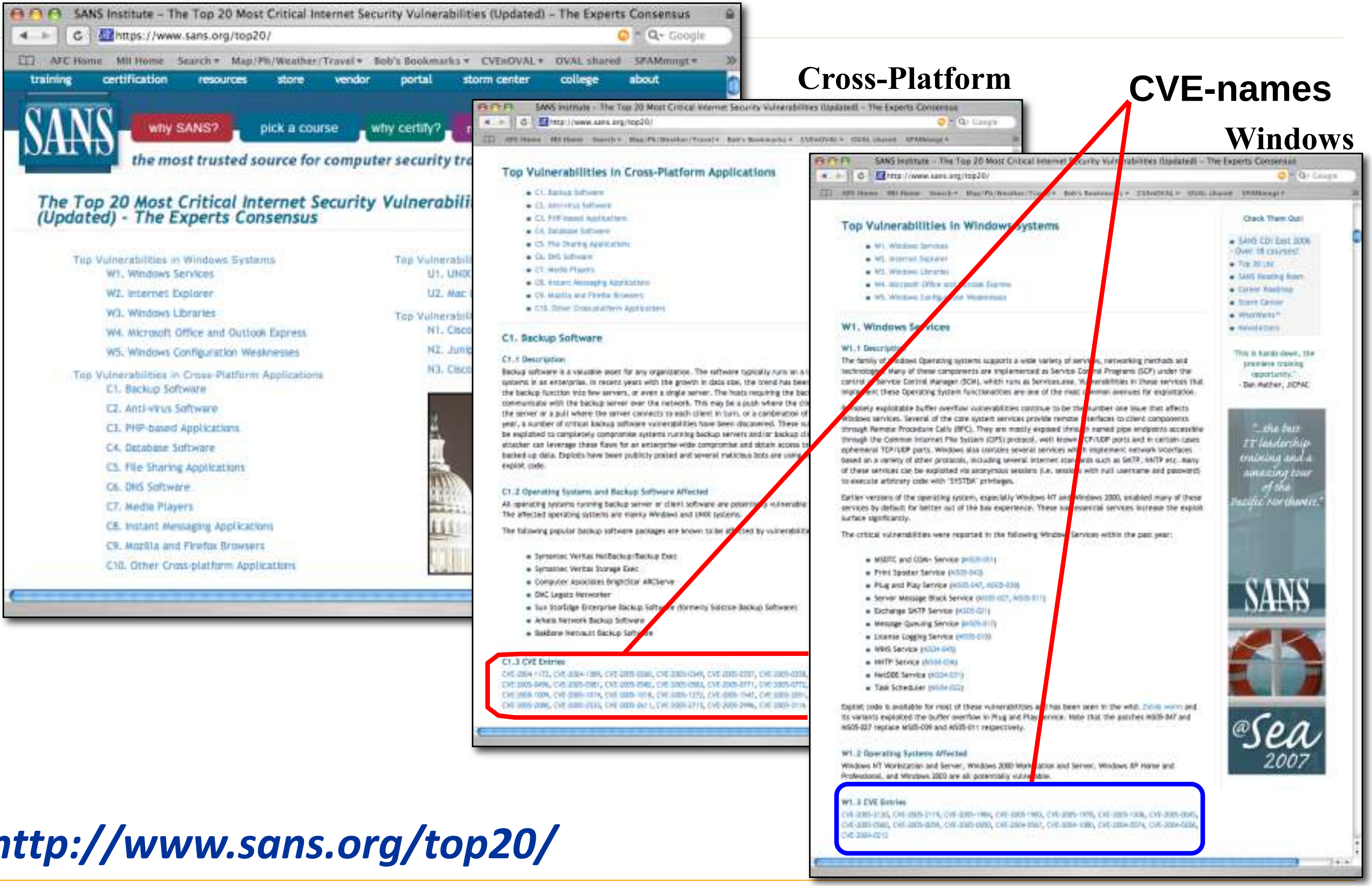
ConfigureSoft

CVE Vendor/Industry Penetration

259 PRODUCTS AND SERVICES FROM 144 ORGANIZATIONS IN 25 COUNTRIES

Avocent
LANDesk
Trustwave
Information Security & Compliance
Certist
GFI
Archer technologies
zoho
CERIAS
SecureInfo
THE INFORMATION ASSURANCE EXPERTS
skybox security
assuria
www.assuria.com
New paradigm
ca
Carnegie Mellon
Software Engineering Institute
McAfee
NetForensics
Soft Run
NSFOCUS
NIST
PatchLink
RAPID 7
天融信 TOPSEC
金诺网安
KINGNET SECURITY INC.
ENTERASYS NETWORKS
Cisco Systems
redhat
QUALYS
APPLICATION SECURITY, INC.
TREND MICRO
Foundstone
STRATEGIC SECURITY
openwall
SANS INSTITUTE
SecurityReason
Our Reason is Security
SAINT
ArcSight
HARRIS
INTERNET SECURITY SYSTEMS
IBM
TENABLE Network Security
SNORT
DragonSoft
www.dragonsoft.com
Intellitactics
symantec.
Critical Watch
Visibility. Measurability. Control
NETCRAFT
nessus
netIQ
Work Smarter.
nCircle
NETWORK SECURITY
(주)나일소프트
NileSOFT Ltd.
LogRADAR
BlueLane
SECURITY DATABASE
KEEP A VIGILANT EYE ON YOUR DEFENSES
NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION
Beyond security
榕基软件
RONGJI
irm
InformationRiskManagement
RUS CERT

The SANS Institute Top 20 List has always used CVE names



SANS Institute - The Top 20 Most Critical Internet Security Vulnerabilities (Updated) - The Experts Consensus

https://www.sans.org/top20/

the most trusted source for computer security tra

The Top 20 Most Critical Internet Security Vulnerabili (Updated) - The Experts Consensus

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players
- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

Top Vulnerabili
U1. UNIX
U2. Mac

Top Vulnerabili
N1. Cisco
N2. Junip
N3. Cisco

Cross-Platform

Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players
- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

C1. Backup Software

C1.1 Description

Backup software is a valuable asset for any organization. The software typically runs on a l systems in an enterprise. In recent years with the growth in data size, the trend has been the backup function into few servers, or even a single server. The hosts requiring the bac communicate with the backup server over the network. This may be a push where the cl the server or a pull where the server connects to each client in turn, or a combination of year, a number of critical backup software vulnerabilities have been discovered. These vu be exploited to completely compromise systems running backup servers and/or backup cl attacker can leverage these flaws for an enterprise-wide compromise and obtain access to backed up data. Exploits have been publicly posted and several malicious bots are using exploit code.

C1.2 Operating Systems and Backup Software Affected

All operating systems running backup server or client software are potentially vulnerable The affected operating systems are mainly Windows and UNIX systems.

The following popular backup software packages are known to be affected by vulnerabiliti

- Symantec Veritas NetBackup/Backup Exec
- Symantec Veritas Storage Exec
- Computer Associates BrightStor ARCServe
- EMC Legato Networker
- Sun StorEdge Enterprise Backup Software (formerly Solstice Backup Software)
- Arkeia Network Backup Software
- BakBone Netvault Backup Software

C1.3 CVE Entries

CVE-2004-1172, CVE-2004-1389, [illegible]

CVE-names

Windows

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

W1. Windows Services

W1.1 Description

The family of Windows Operating systems supports a wide variety of services, networking methods and technologies. Many of these components are implemented as Service Control Programs (SCP) under the control of Service Control Manager (SCM), which runs as Services.exe. Vulnerabilities in these services that implement these Operating System functionalities are one of the most common avenues for exploitation.

Remotely exploitable buffer overflow vulnerabilities continue to be the number one issue that affects Windows services. Several of the core system services provide remote interfaces to client components through Remote Procedure Calls (RPC). They are mostly exposed through named pipe endpoints accessible through the Common Internet File System (CIFS) protocol, well known TCP/UDP ports and in certain cases ephemeral TCP/UDP ports. Windows also contains several services which implement network interfaces based on a variety of other protocols, including several Internet standards such as SMTP, NNTP etc. Many of these services can be exploited via anonymous sessions (i.e. sessions with null username and password) to execute arbitrary code with "SYSTEM" privileges.

Earlier versions of the operating system, especially Windows NT and Windows 2000, enabled many of these services by default for better out of the box experience. These non-essential services increase the exploit surface significantly.

The critical vulnerabilities were reported in the following Windows Services within the past year:

- MSDTC and COM+ Service (MS05-051)
- Print Spooler Service (MS05-043)
- Plug and Play Service (MS05-047, MS05-039)
- Server Message Block Service (MS05-027, MS05-011)
- Exchange SMTP Service (MS05-021)
- Message Queuing Service (MS05-017)
- License Logging Service (MS05-010)
- WINS Service (MS04-045)
- NNTP Service (MS04-036)
- NetDDE Service (MS04-031)
- Task Scheduler (MS04-022)

Exploit code is available for most of these vulnerabilities and has been seen in the wild. Zotob worm and its variants exploited the buffer overflow in Plug and Play service. Note that the patches MS05-047 and MS05-027 replace MS05-039 and MS05-011 respectively.

W1.2 Operating Systems Affected

Windows NT Workstation and Server, Windows 2000 Workstation and Server, Windows XP Home and Professional, and Windows 2003 are all potentially vulnerable.

W1.3 CVE Entries

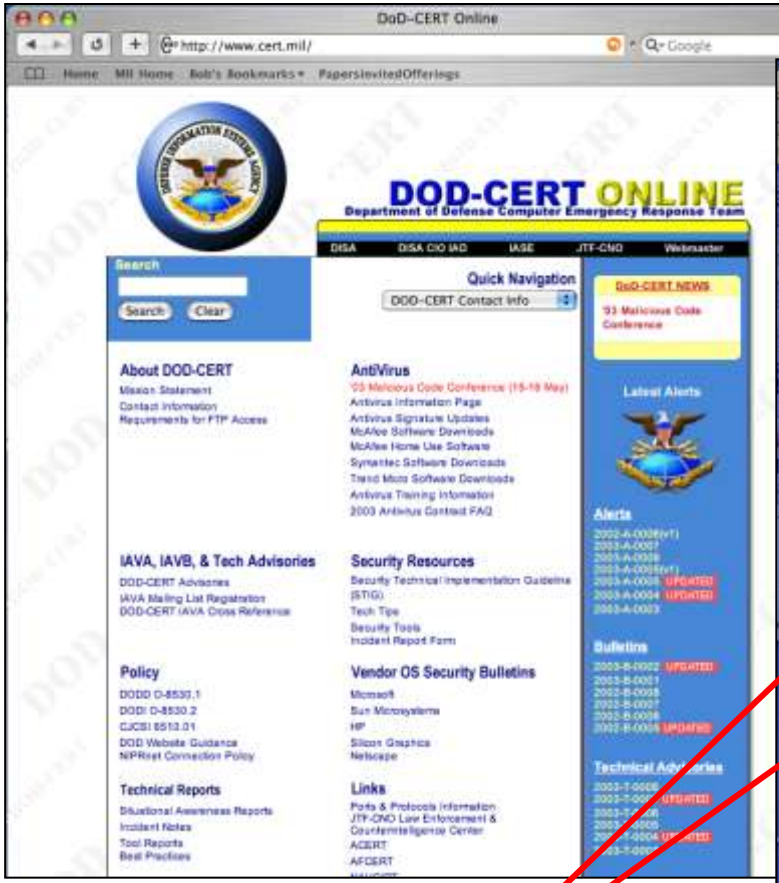
[illegible]

Check Them Out!
SANS CDI East 2006 - Over 18 courses!
Top 20 List
SANS Reading Room
Career Roadmap
Storm Center
WhatWorks
Newsletters
"This is hands-down, the premiere training opportunity." - Dan Mather, JICPAC
"...the best IT leadership training and a amazing tour of the Pacific Northwest."
SANS
@Sea 2007

http://www.sans.org/top20/

Version 6.01 Released Oct 12, 2006

DoD's Information Assurance Vulnerability Alerts (IAVAs) use CVE names



About DOD-CERT
Mission Statement
Contact Information
Requirements for FTP Access

AntiVirus
'03 Malicious Code Conference (15-16 May)
Antivirus Information Page
Antivirus Signature Updates
McAfee Software Downloads
McAfee Home Use Software
Symantec Software Downloads
Trend Micro Software Downloads
Antivirus Training Information
2003 Antivirus Contract FAQ

IAVA, IAVB, & Tech Advisories
DOD-CERT Advisories
IAVA Mailing List Registration
DOD-CERT IAVA Cross Reference

Security Resources
Security Technical Implementation Guideline (STIG)
Tech Tips
Security Tools
Incident Report Form

Policy
DODD O-8530.1
DODI O-8530.2
CJCSI 6510.01
DOD Website Guidance
NIPRnet Connection Policy

Vendor OS Security Bulletins
Microsoft
Sun Microsystems
HP
Silicon Graphics
Netscape

Technical Reports
Situational Awareness Reports
Incident Notes
Tool Reports
Best Practices

Links
Ports & Protocols Information
JTF-CND Law Enforcement & Counterintelligence Center
ACERT
AFCERT

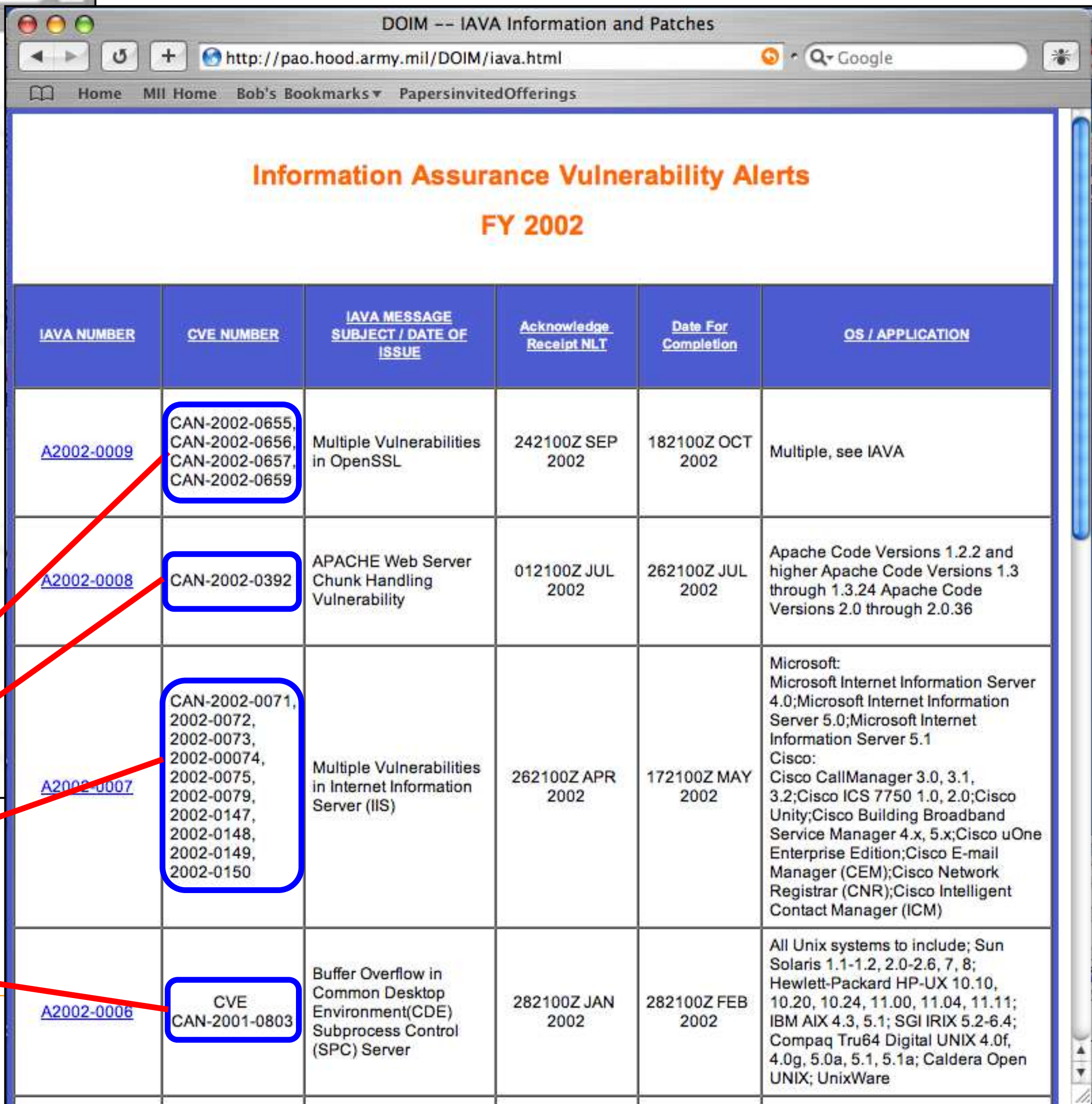
DoD-CERT NEWS
'03 Malicious Code Conference

Latest Alerts

Alerts
2002-A-0008(v1)
2003-A-0007
2003-A-0006
2003-A-0005(v1)
2003-A-0005 UPDATED
2003-A-0004 UPDATED
2003-A-0003

Bulletins
2003-B-0002 UPDATED
2003-B-0001
2002-B-0008
2002-B-0007
2002-B-0006
2002-B-0005 UPDATED

Technical Advisories
2003-T-0008
2003-T-0007 UPDATED
2003-T-0006
2003-T-0005
2003-T-0004 UPDATED
2003-T-0003


DOIM -- IAVA Information and Patches
http://pao.hood.army.mil/DOIM/iava.html
Google
Home
Mil Home
Bob's Bookmarks
PapersinvitedOfferings

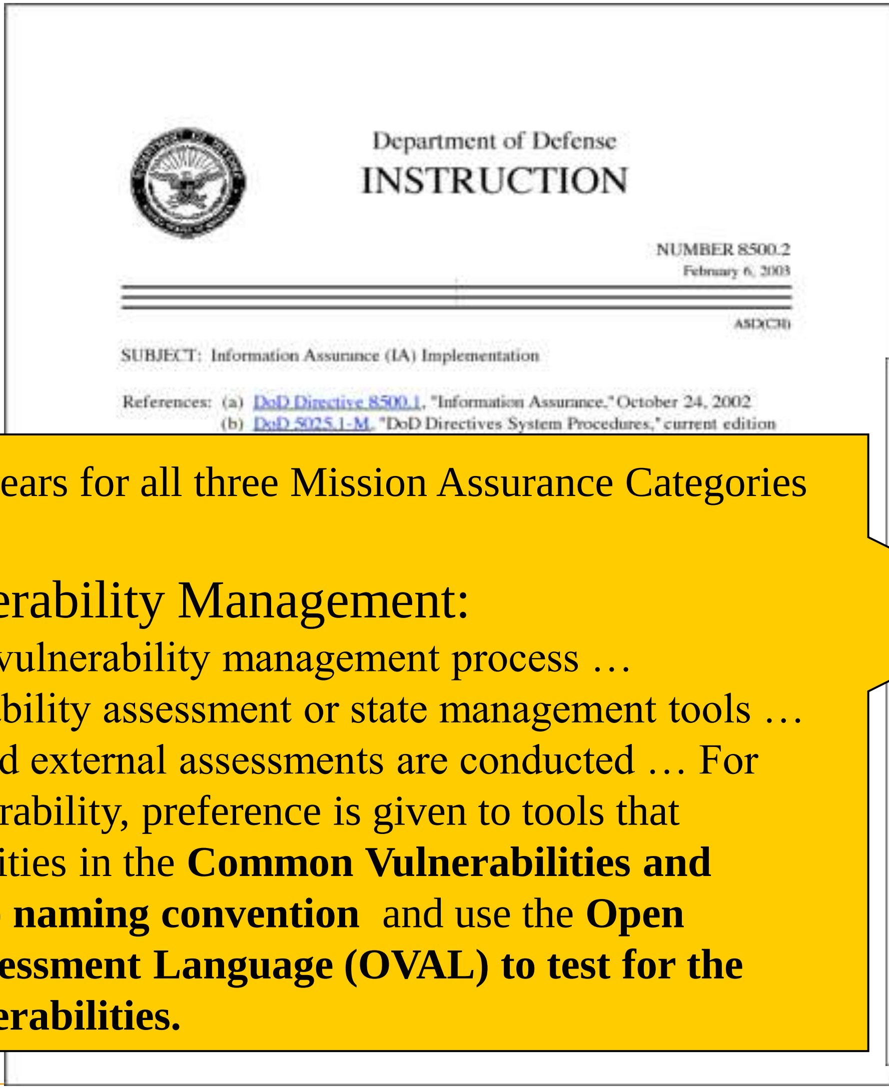
Information Assurance Vulnerability Alerts

FY 2002

IAVA NUMBER	CVE NUMBER	IAVA MESSAGE SUBJECT / DATE OF ISSUE	Acknowledge Receipt NLT	Date For Completion	OS / APPLICATION
A2002-0009	CAN-2002-0655, CAN-2002-0656, CAN-2002-0657, CAN-2002-0659	Multiple Vulnerabilities in OpenSSL	242100Z SEP 2002	182100Z OCT 2002	Multiple, see IAVA
A2002-0008	CAN-2002-0392	APACHE Web Server Chunk Handling Vulnerability	012100Z JUL 2002	262100Z JUL 2002	Apache Code Versions 1.2.2 and higher Apache Code Versions 1.3 through 1.3.24 Apache Code Versions 2.0 through 2.0.36
A2002-0007	CAN-2002-0071, 2002-0072, 2002-0073, 2002-00074, 2002-0075, 2002-0079, 2002-0147, 2002-0148, 2002-0149, 2002-0150	Multiple Vulnerabilities in Internet Information Server (IIS)	262100Z APR 2002	172100Z MAY 2002	Microsoft: Microsoft Internet Information Server 4.0;Microsoft Internet Information Server 5.0;Microsoft Internet Information Server 5.1 Cisco: Cisco CallManager 3.0, 3.1, 3.2;Cisco ICS 7750 1.0, 2.0;Cisco Unity;Cisco Building Broadband Service Manager 4.x, 5.x;Cisco uOne Enterprise Edition;Cisco E-mail Manager (CEM);Cisco Network Registrar (CNR);Cisco Intelligent Contact Manager (ICM)
A2002-0006	CVE CAN-2001-0803	Buffer Overflow in Common Desktop Environment(CDE) Subprocess Control (SPC) Server	282100Z JAN 2002	282100Z FEB 2002	All Unix systems to include; Sun Solaris 1.1-1.2, 2.0-2.6, 7, 8; Hewlett-Packard HP-UX 10.10, 10.20, 10.24, 11.00, 11.04, 11.11; IBM AIX 4.3, 5.1; SGI IRIX 5.2-6.4; Compaq Tru64 Digital UNIX 4.0f, 4.0g, 5.0a, 5.1, 5.1a; Caldera Open UNIX; UnixWare

CVE-names

DoD 8500.2 IA Implementation Instruction gives *preference* to products supporting CVE & OVAL



Department of Defense

INSTRUCTION

NUMBER 8500.2
February 6, 2003

ASD(C3I)

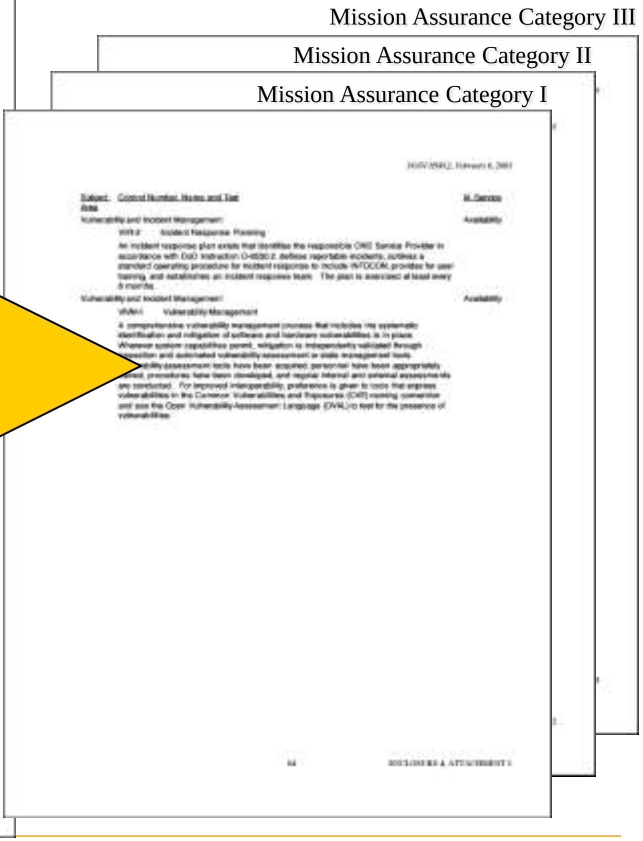
SUBJECT: Information Assurance (IA) Implementation

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(b) DoD 5025.1-M, "DoD Directives System Procedures," current edition

The following appears for all three Mission Assurance Categories of DOD systems:

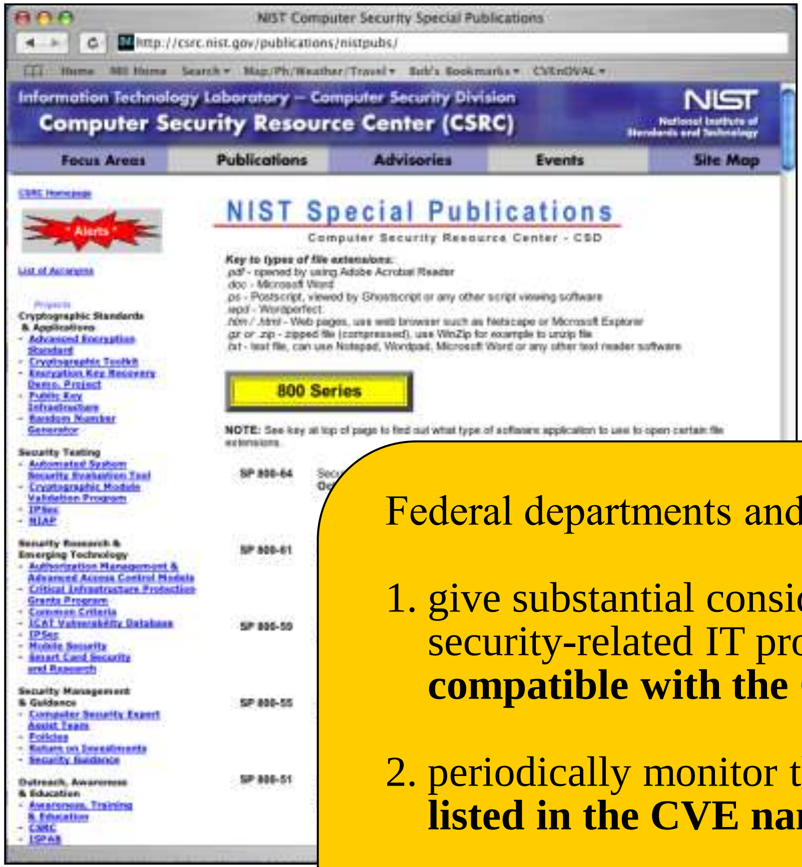
VIVM-1 Vulnerability Management:

A comprehensive vulnerability management process … automated vulnerability assessment or state management tools … regular internal and external assessments are conducted … For improved interoperability, preference is given to tools that express vulnerabilities in the **Common Vulnerabilities and Exposures (CVE) naming convention** and use the **Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.**


Mission Assurance Category III
Mission Assurance Category II
Mission Assurance Category I

http://www.nstissc.gov/html/library.htm

National Institute of Standards and Technology (NIST): Policy on the Use of CVE and CVE-Compatible products



NIST Computer Security Special Publications

http://csrc.nist.gov/publications/nistpubs/

Information Technology Laboratory – Computer Security Division

Computer Security Resource Center (CSRC)

NIST National Institute of Standards and Technology

Projects

Cryptographic Standards & Applications
- Advanced Encryption Standard
- Cryptographic Toolkit
- Encryption Key Recovery Demo. Project
- Public Key Infrastructure
- Random Number Generator

Security Testing
- Automated System Security Evaluation Tool
- Cryptographic Module Validation Program
- IPSec
- NIAP

Security Research & Emerging Technology
- Authorization Management & Advanced Access Control Models
- Critical Infrastructure Protection Grants Program
- Common Criteria
- ICAT Vulnerability Database
- IPSec
- Mobile Security
- Smart Card Security and Research

Security Management & Guidance
- Computer Security Expert Assist Team
- Policies
- Return on Investments
- Security Guidance

Outreach, Awareness & Education
- Awareness, Training & Education
- CSRC
- ISPAB

NIST Special Publications

Computer Security Resource Center - CSD

Key to types of file extensions:
.pdf - opened by using Adobe Acrobat Reader
.doc - Microsoft Word
.ps - Postscript, viewed by Ghostscript or any other script viewing software
.wpd - Wordperfect
.htm / .html - Web pages, use web browser such as Netscape or Microsoft Explorer
.gz or .zip - zipped file (compressed), use WinZip for example to unzip file
.txt - text file, can use Notepad, Wordpad, Microsoft Word or any other text reader software

800 Series

NOTE: See key at top of page to find out what type of software application to use to open certain file extensions.

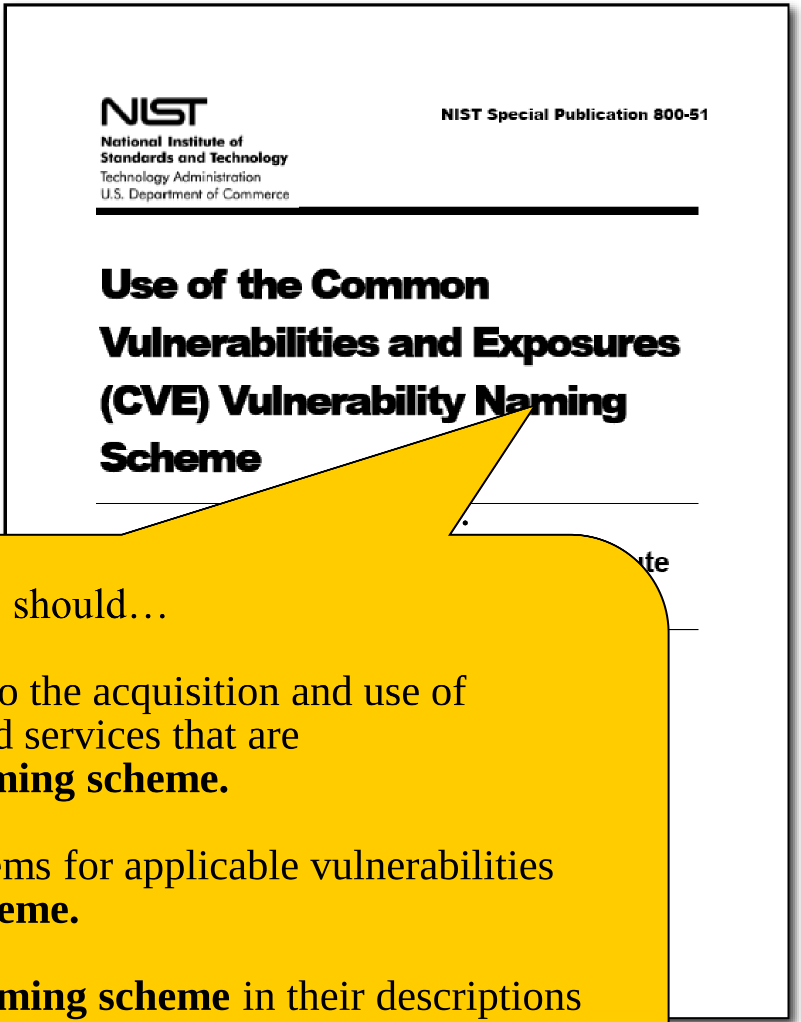
SP 800-64

SP 800-61

SP 800-59

SP 800-55

SP 800-51



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

NIST Special Publication 800-51

Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme

Federal departments and agencies should…

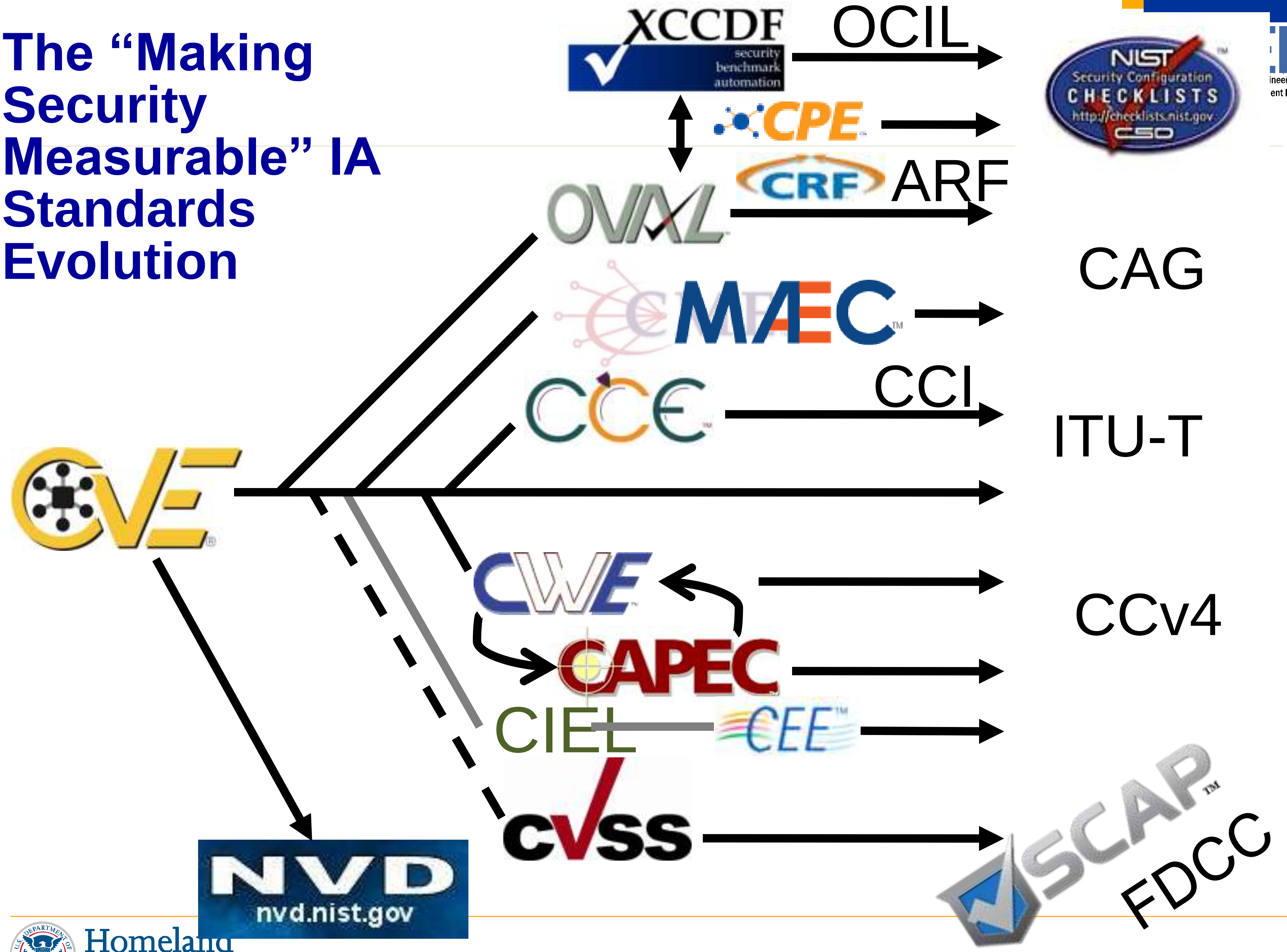
1. give substantial consideration to the acquisition and use of security-related IT products and services that are **compatible with the CVE naming scheme.**

2. periodically monitor their systems for applicable vulnerabilities **listed in the CVE naming scheme.**

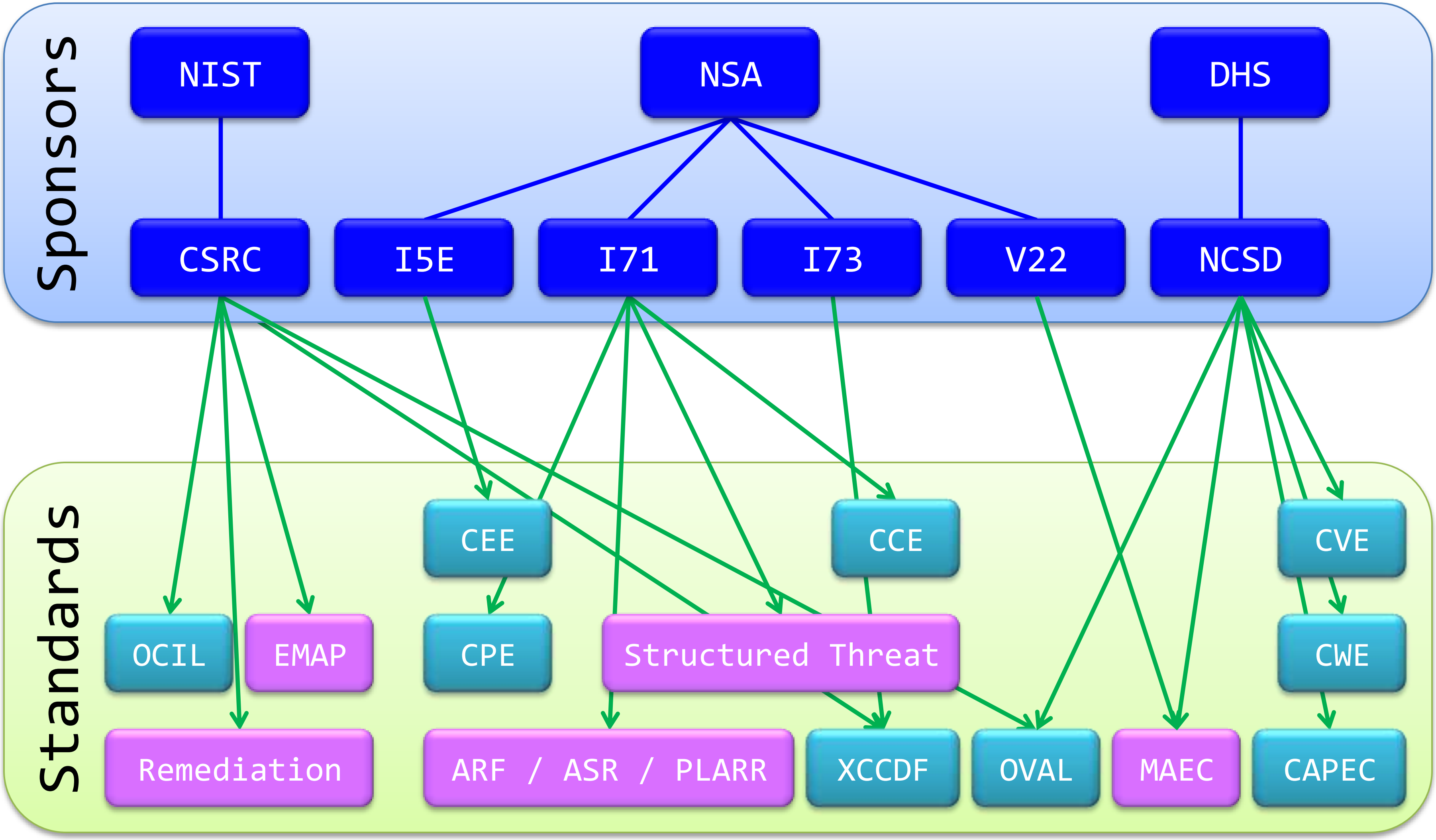
3. **use the CVE vulnerability naming scheme** in their descriptions and communications of vulnerabilities

http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf

The “Making Security Measurable” IA Standards Evolution



Funders of MITRE's work on the "Making Security Measurable" IA Standards Efforts



http://www.first.org/cvss/

The Common Vulnerability Scoring System (CVSS) v2

Original Author: Gavin Reid, Cisco

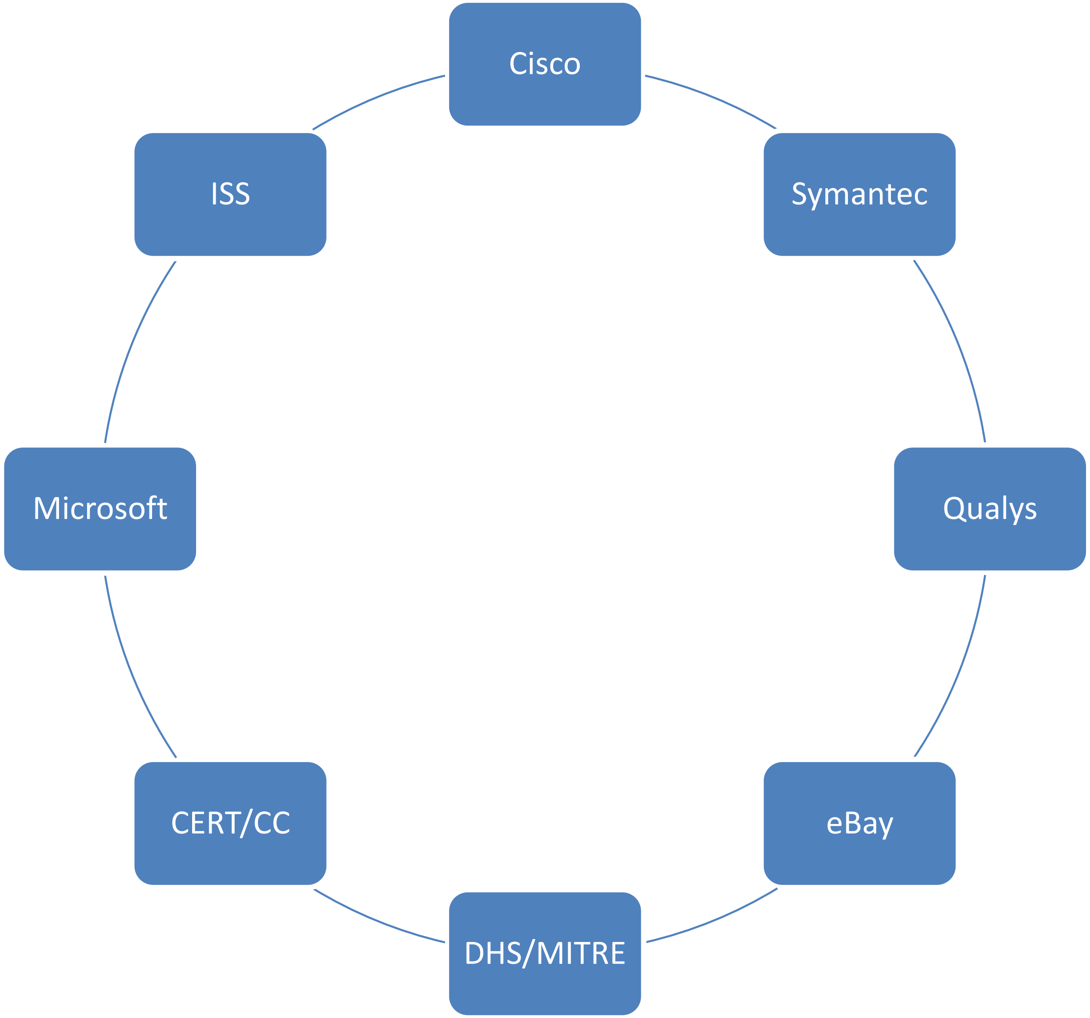
Agenda

- Introduction and overview of CVSS
- Why CVSS?
- Internals
- Scoring
- Roadmap
- Closing comments and questions

Overview

- **Common Vulnerability Scoring System (CVSS)**
- **A universal language to convey vulnerability severity and help determine urgency and priority of response**
- **Solves problem of multiple, incompatible scoring systems in use today**
- **Initially a NIAC project**
  - Subgroup of the global Vulnerability Disclosure Framework WG
  - Now under the custodial care of FIRST-SIG
- **Usable, understandable, and dissectible by anyone**
- **Open**
- **v2 released (June 20th 2007)**

A joint NIAC effort



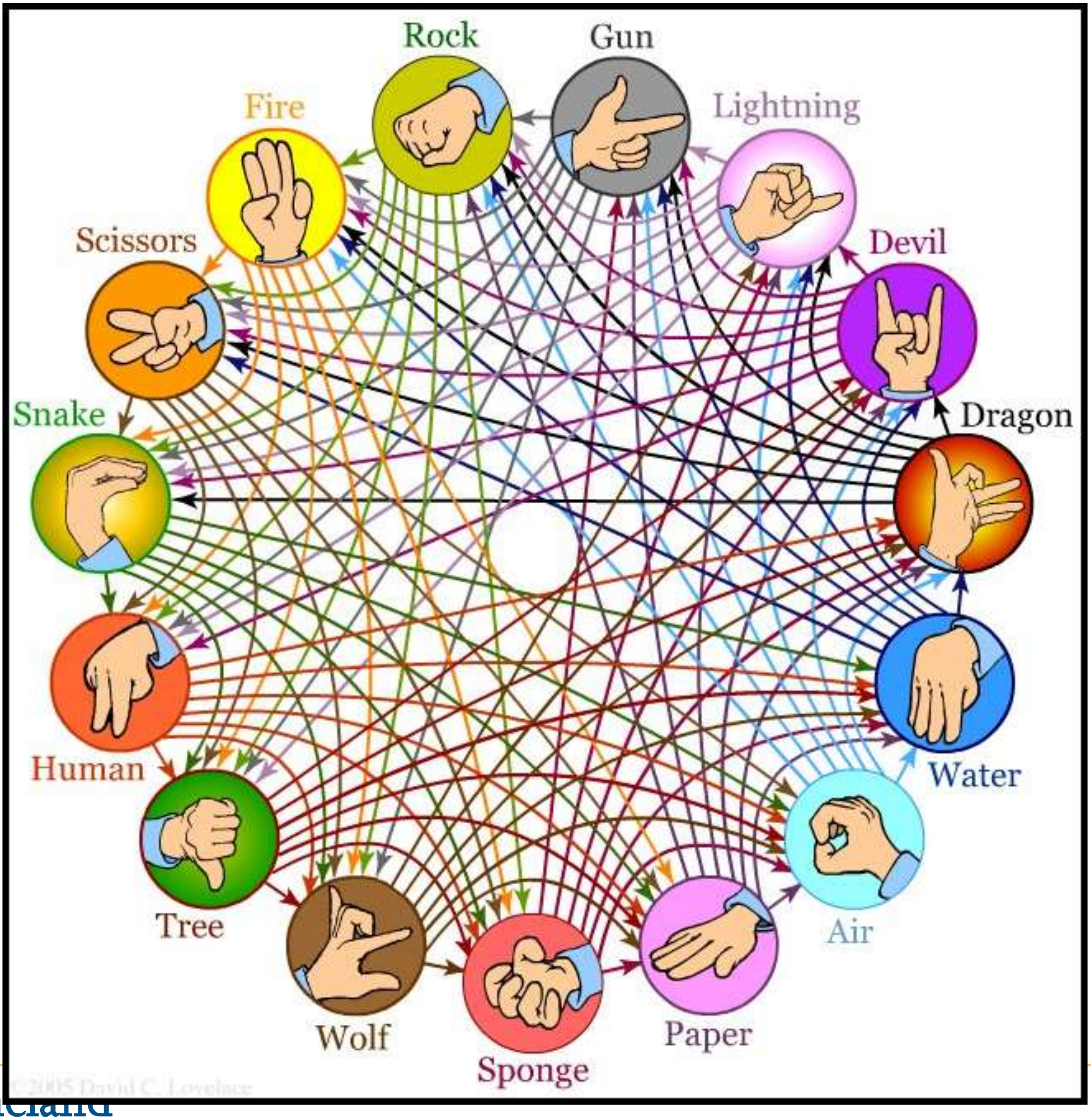
Early Adopters

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
IBM
symantec.
QUALYS
ON DEMAND SECURITY
U.S. DEPARTMENT OF HOMELAND SECURITY
hp
invent
ArcSight
assuria
skype
McAfee
skybox
security
secure elements
audit. evaluate. comply.
nCircle
Proactive Network Security
BIGFIX
redseal
SYSTEMS
E-SECURE-IT
ALERT & EARLY WARNING SYSTEM
WWW.E-SECURE-IT.COM
CISCO
SECURITY DATABASE.
KEEP A VIGILANT EYE ON YOUR DEFENSES
Security Risk Management Solutions
netVigilance
assurance has arrived
ORACLE
ThreatGuard
TENABLE
Network Security
NIST

Why CVSS?

- Different Organizations
  - Vendors (response)
  - Coordinators (notification, coordination)
  - Reporters (research, discovery)
  - Users (mitigation)
- Different roles, motivations, priorities, resources, etc
- We need a common way to communicate!
- Set an industry example on alert disclosure

Pre-CVSS


Rock
Gun
Lightning
Devil
Dragon
Water
Air
Paper
Sponge
Wolf
Tree
Human
Snake
Scissors
Fire
©2005 David C. Lovelace

Vendor Scoring: Microsoft

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Coordinator Scoring: CERT/CC

The metric value is a number between 0 and 180 that assigns an approximate severity to the vulnerability. This number considers several factors, including:

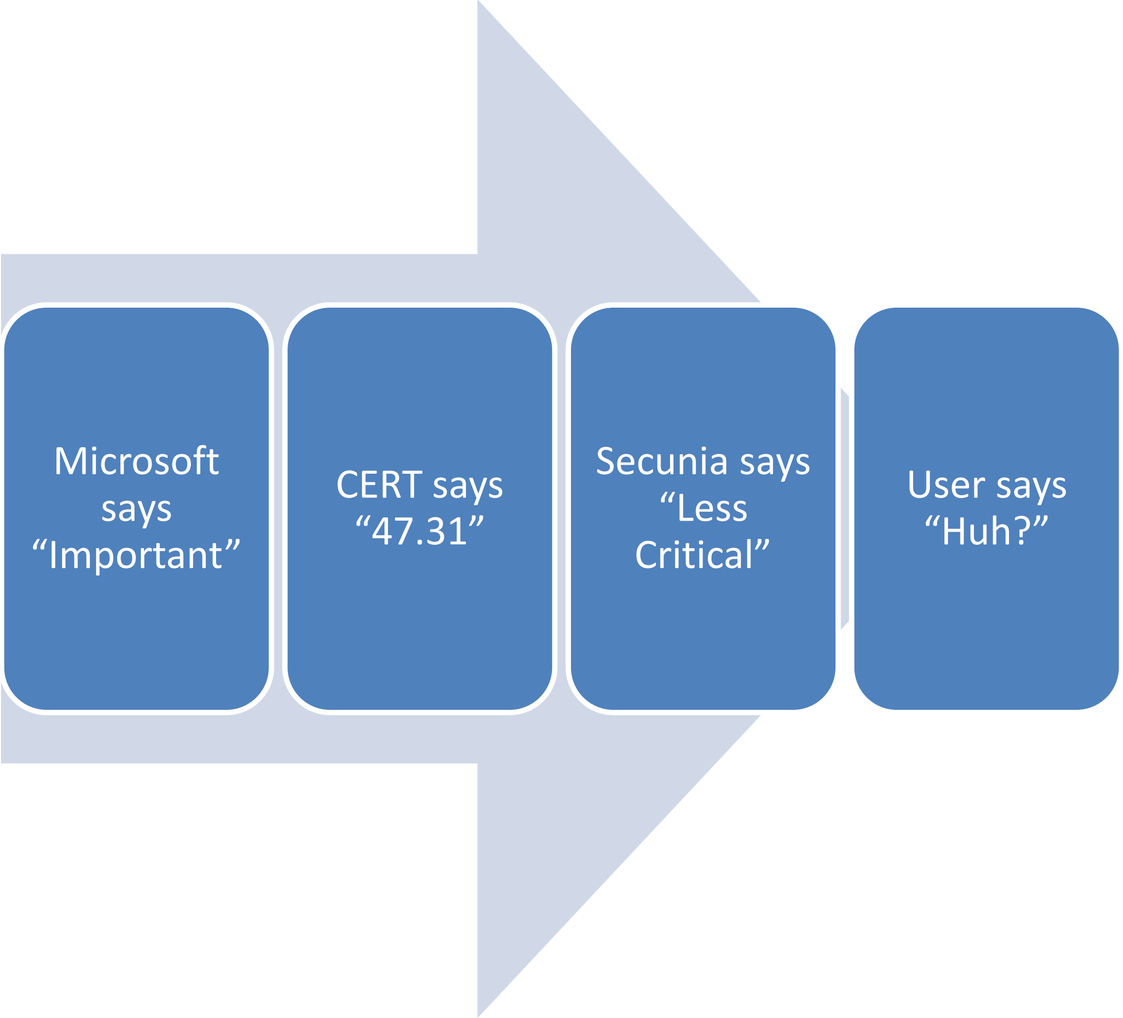
Q1 Is information about the vulnerability widely available or known?
Q2 Is the vulnerability being exploited in the incidents reported?
Q3 Is the Internet Infrastructure at risk because of this vulnerability?
Q4 How many systems on the Internet are at risk from this vulnerability?
Q5 What is the impact of exploiting the vulnerability?
Q6 How easy is it to exploit the vulnerability?
Q7 What are the preconditions required to exploit the vulnerability?

```
3 * (Q1 + Q2 + Q3) * (Q4 * Q5 * Q6 * Q7) / (20^4)
```

Researcher Scoring: Secunia

Rating	Definition
Extremely Critical	Typically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild.
Highly Critical	As Above, no known exploits
Moderately Critical	As Above, but DoS only or requiring user interaction
Less Critical	XSS, privilege escalation, sensitive data exposure
Not Critical	Very limited privilege escalation, locally exploitable DoS, non-sensitive data exposure

And the User…?



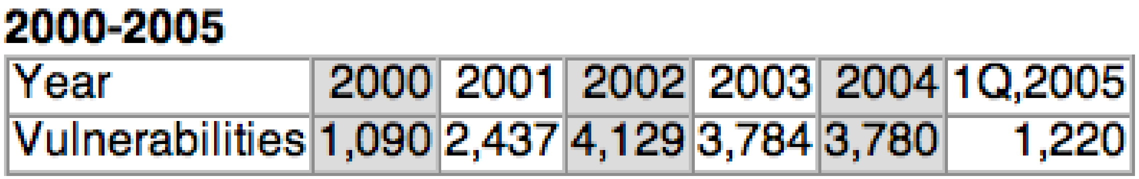
Microsoft says “Important”

CERT says “47.31”

Secunia says “Less Critical”

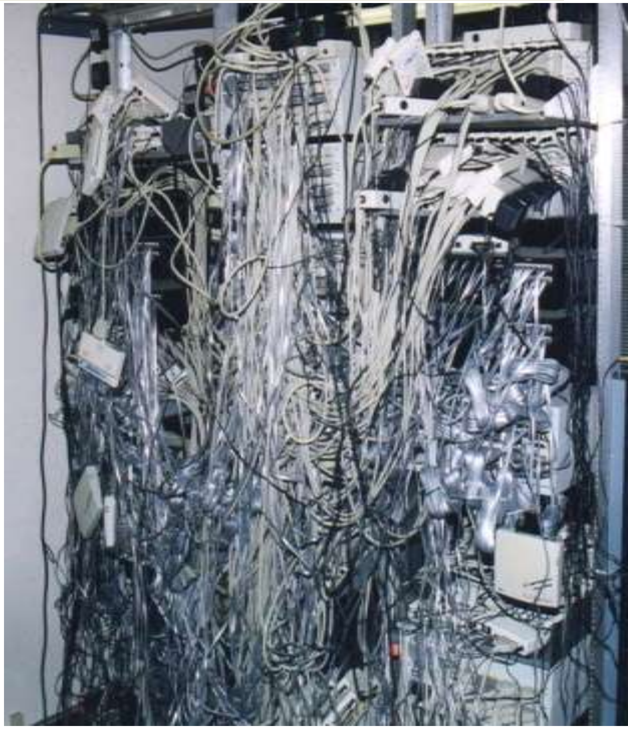
User says “Huh?”

The Busy Security Operations Guy



2000-2005

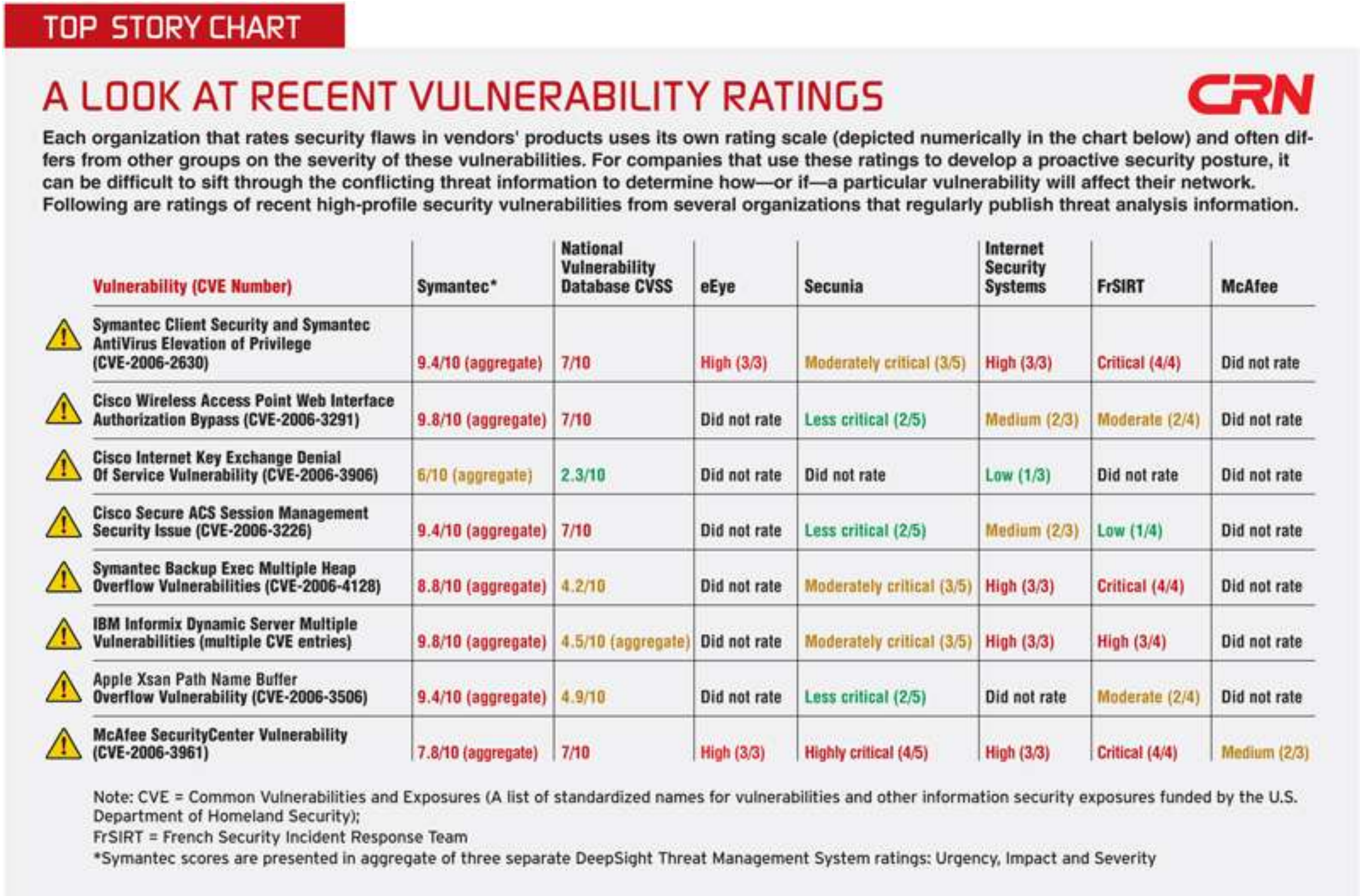
Year	2000	2001	2002	2003	2004	1Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	1,220



What does it mean to have 4,129 vulnerabilities reported in 2002?

- Read the descriptions
  - 4,129 vulnerabilities * 15 minutes = 129 days
- Affected by 10% of the vulnerabilities?
- Install patches on one system
  - 413 vulnerabilities * 1 hour = 52 days
- Reading reports and patching a single system costs 129 + 52 = 181 days
- Which vulnerability should I patch first? Remote root in DNS? Web server? Desktop systems? DoS affecting routing infrastructure?

Scoring Discrepancy Chart



TOP STORY CHART

A LOOK AT RECENT VULNERABILITY RATINGS

CRN

Each organization that rates security flaws in vendors' products uses its own rating scale (depicted numerically in the chart below) and often differs from other groups on the severity of these vulnerabilities. For companies that use these ratings to develop a proactive security posture, it can be difficult to sift through the conflicting threat information to determine how—or if—a particular vulnerability will affect their network. Following are ratings of recent high-profile security vulnerabilities from several organizations that regularly publish threat analysis information.

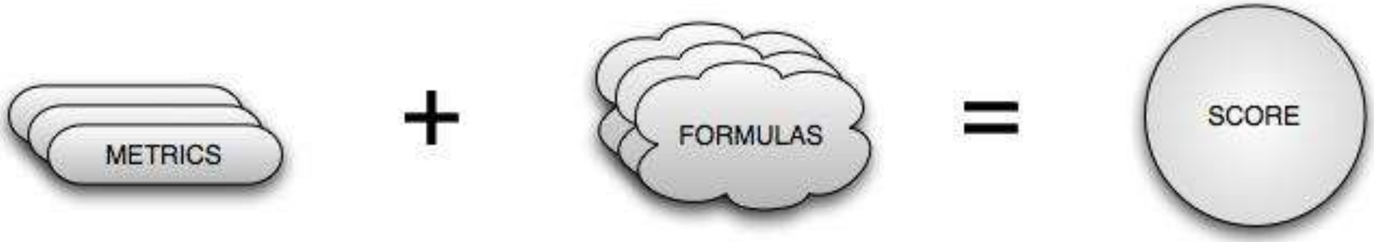
Vulnerability (CVE Number)	Symantec*	National Vulnerability Database CVSS	eEye	Secunia	Internet Security Systems	FrSIRT	McAfee
⚠ Symantec Client Security and Symantec AntiVirus Elevation of Privilege (CVE-2006-2630)	9.4/10 (aggregate)	7/10	High (3/3)	Moderately critical (3/5)	High (3/3)	Critical (4/4)	Did not rate
⚠ Cisco Wireless Access Point Web Interface Authorization Bypass (CVE-2006-3291)	9.8/10 (aggregate)	7/10	Did not rate	Less critical (2/5)	Medium (2/3)	Moderate (2/4)	Did not rate
⚠ Cisco Internet Key Exchange Denial Of Service Vulnerability (CVE-2006-3906)	6/10 (aggregate)	2.3/10	Did not rate	Did not rate	Low (1/3)	Did not rate	Did not rate
⚠ Cisco Secure ACS Session Management Security Issue (CVE-2006-3226)	9.4/10 (aggregate)	7/10	Did not rate	Less critical (2/5)	Medium (2/3)	Low (1/4)	Did not rate
⚠ Symantec Backup Exec Multiple Heap Overflow Vulnerabilities (CVE-2006-4128)	8.8/10 (aggregate)	4.2/10	Did not rate	Moderately critical (3/5)	High (3/3)	Critical (4/4)	Did not rate
⚠ IBM Informix Dynamic Server Multiple Vulnerabilities (multiple CVE entries)	9.8/10 (aggregate)	4.5/10 (aggregate)	Did not rate	Moderately critical (3/5)	High (3/3)	High (3/4)	Did not rate
⚠ Apple Xsan Path Name Buffer Overflow Vulnerability (CVE-2006-3506)	9.4/10 (aggregate)	4.9/10	Did not rate	Less critical (2/5)	Did not rate	Moderate (2/4)	Did not rate
⚠ McAfee SecurityCenter Vulnerability (CVE-2006-3961)	7.8/10 (aggregate)	7/10	High (3/3)	Highly critical (4/5)	High (3/3)	Critical (4/4)	Medium (2/3)

Note: CVE = Common Vulnerabilities and Exposures (A list of standardized names for vulnerabilities and other information security exposures funded by the U.S. Department of Homeland Security);
FrSIRT = French Security Incident Response Team
*Symantec scores are presented in aggregate of three separate DeepSight Threat Management System ratings: Urgency, Impact and Severity

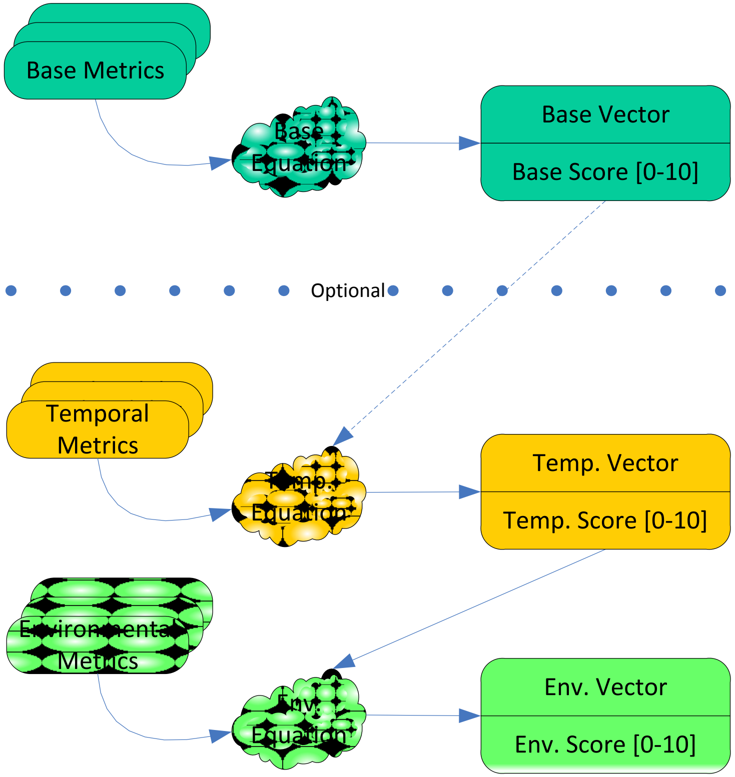
How does CVSS work?

Metrics and formulas yield a score

That's all!



CVSS (Metrics View)



Base Metric Group

- Most fundamental qualities of a vulnerability
- Do not change; “Immutable”
- Intrinsic attributes of a vulnerability
- 6 Base metrics

Access Complexity

Authentication

Impacts (CIA)

Base Metrics

Access Vector (AV)

Measures whether a vulnerability is exploitable locally or remotely

Local (L): The vulnerability is only exploitable locally

Adjacent Network (A): The vulnerability must be staged from either the broadcast or collision domain of the vulnerable software

Network (N): The vulnerability is exploitable remotely (and possibly locally as well) An example of a network attack is an RPC buffer overflow.

Base Metrics

Access Complexity (AC)

Measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system

High (H) : Specialized access conditions exist. For example: In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS). The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions. The vulnerable configuration is seen very rarely in practice. - If a race condition exists, the window is very narrow.

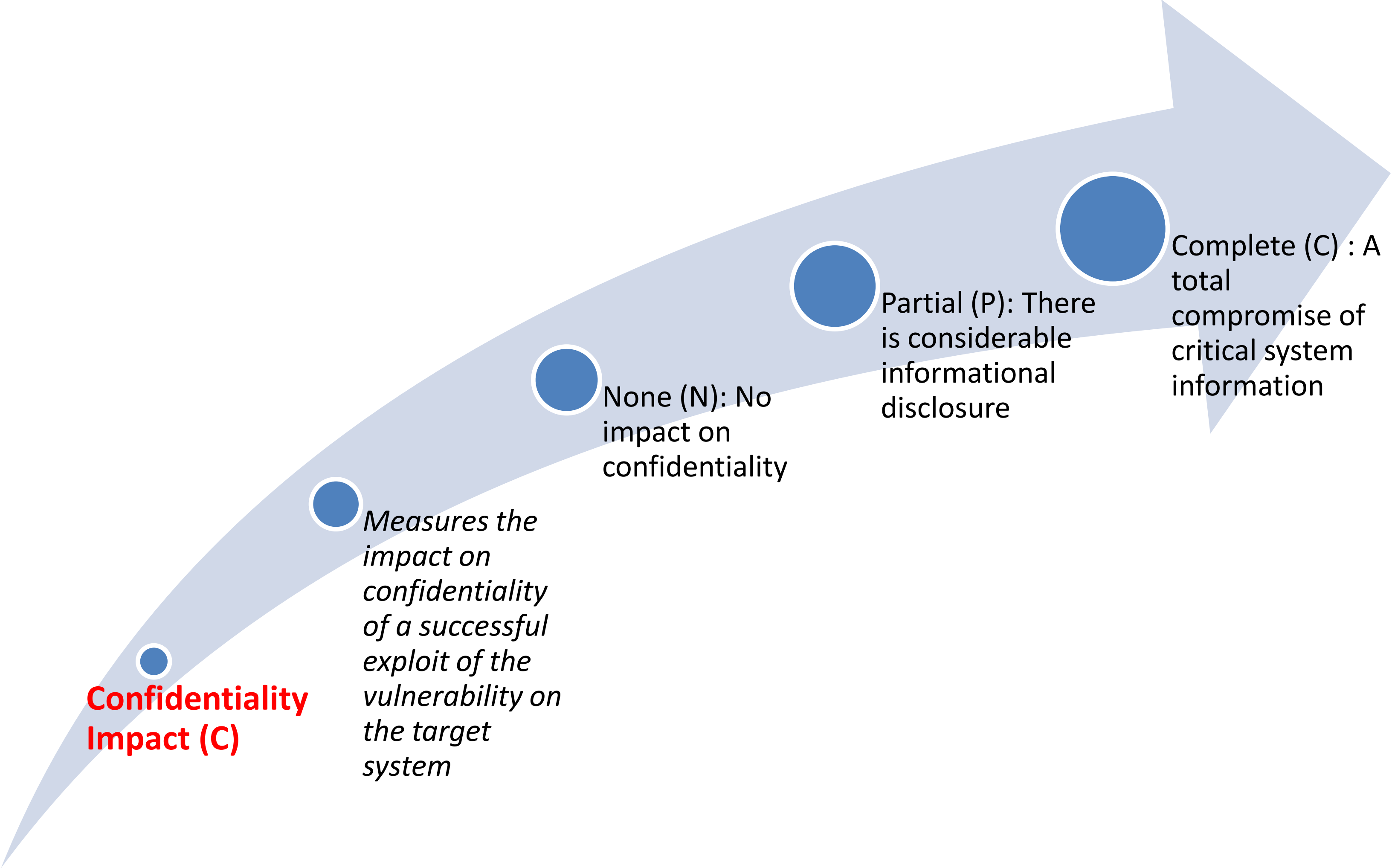
Medium (M) : The access conditions are somewhat specialized; the following are examples: The attacking party is limited to a group of systems or users at some level of authorization. The affected configuration is non-default, and is not commonly configured. The attack requires a small amount of social engineering that might occasionally fool cautious

Low (L) : Specialized access conditions or extenuating circumstances do not exist. The following are examples: The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server). The attack can be performed manually and requires little skill or additional information gathering. Used default configuration

Authentication (Au)

- Measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability
- Multiple (M) Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system.
- Single (S) The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).
- None (N) Authentication is not required to exploit the vulnerability.

Base Metrics



Confidentiality Impact (C)

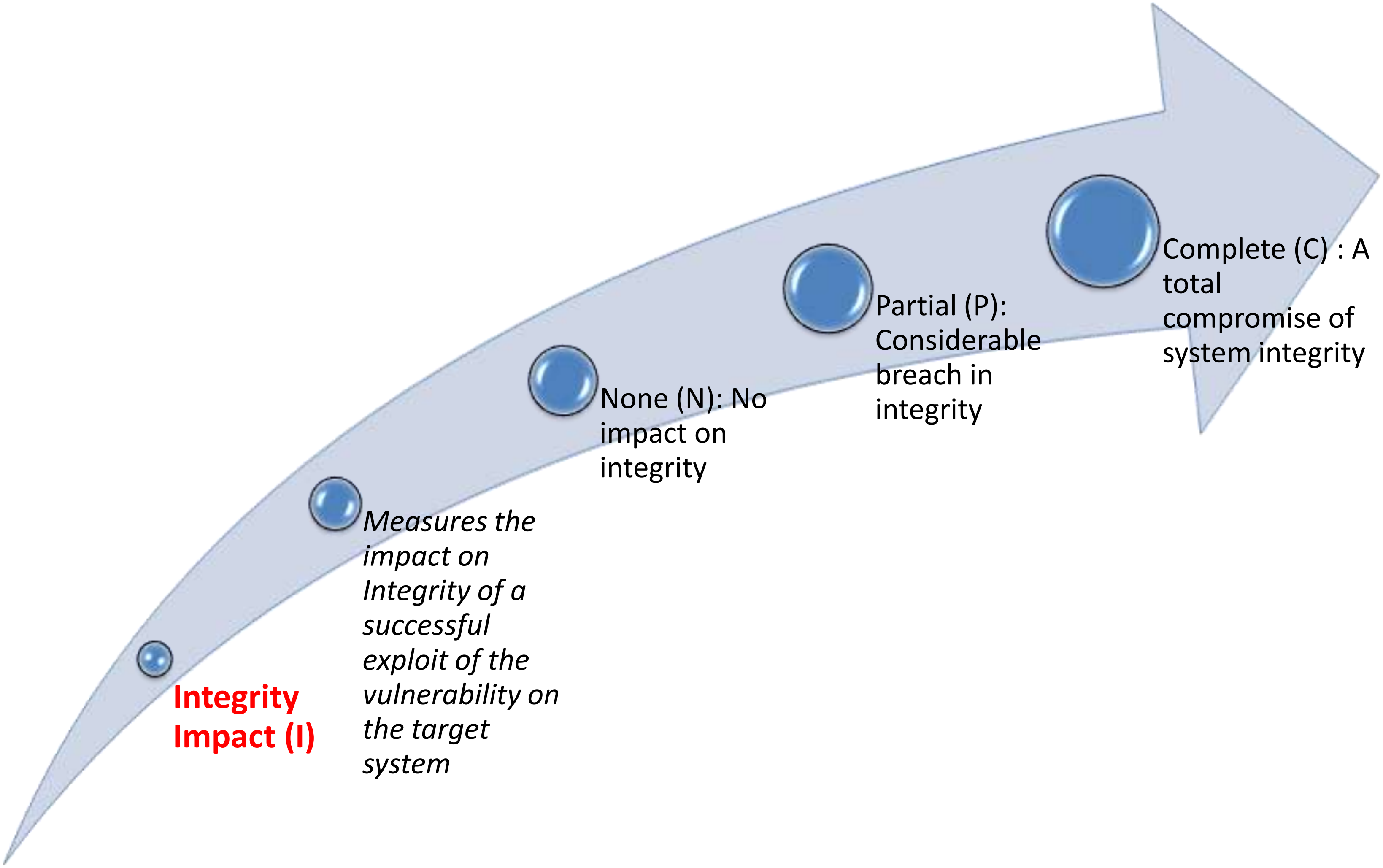
Measures the impact on confidentiality of a successful exploit of the vulnerability on the target system

None (N): No impact on confidentiality

Partial (P): There is considerable informational disclosure

Complete (C) : A total compromise of critical system information

Base Metrics



Integrity Impact (I)

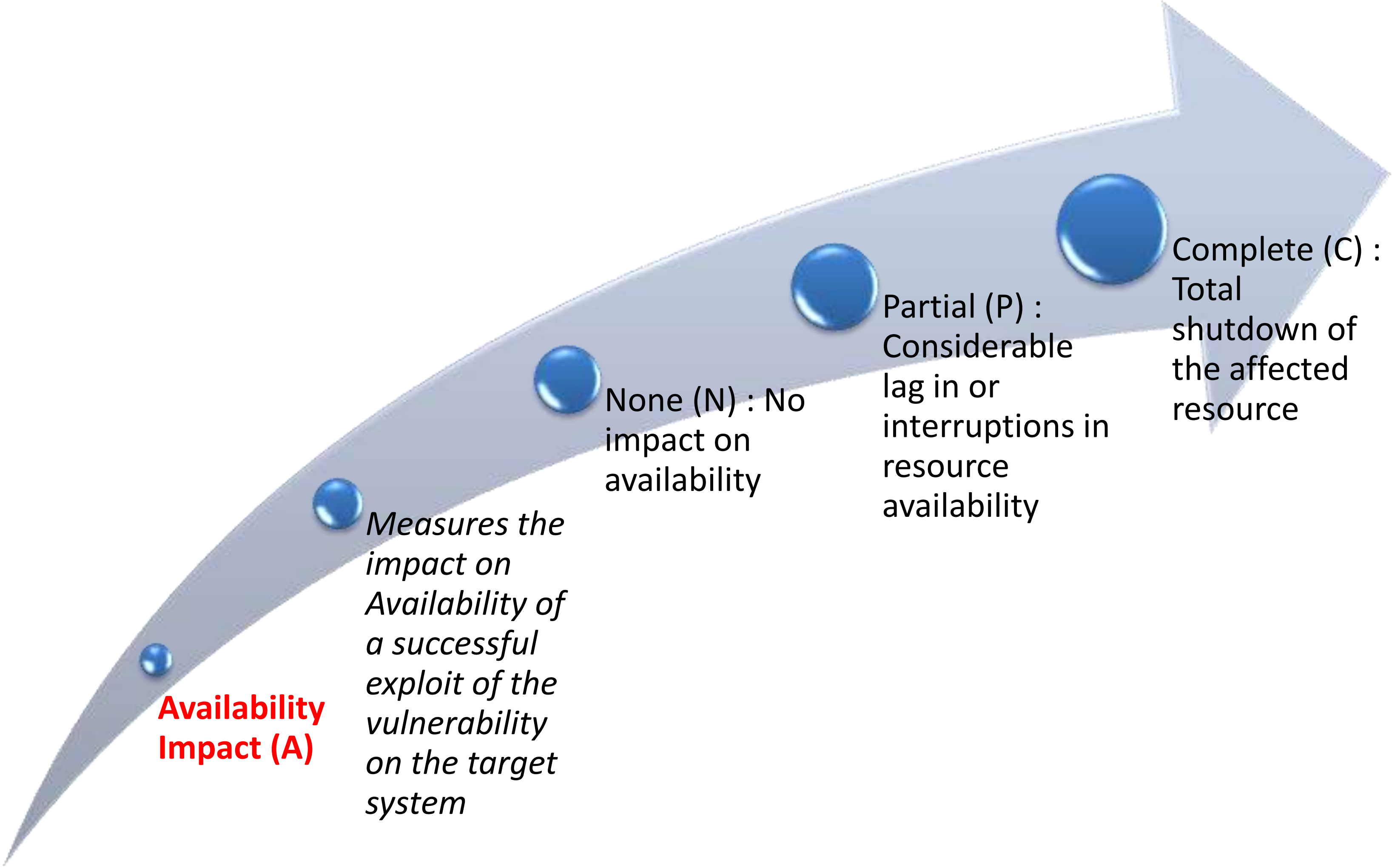
Measures the impact on Integrity of a successful exploit of the vulnerability on the target system

None (N): No impact on integrity

Partial (P): Considerable breach in integrity

Complete (C) : A total compromise of system integrity

Base Metrics



Availability Impact (A)

Measures the impact on Availability of a successful exploit of the vulnerability on the target system

None (N) : No impact on availability

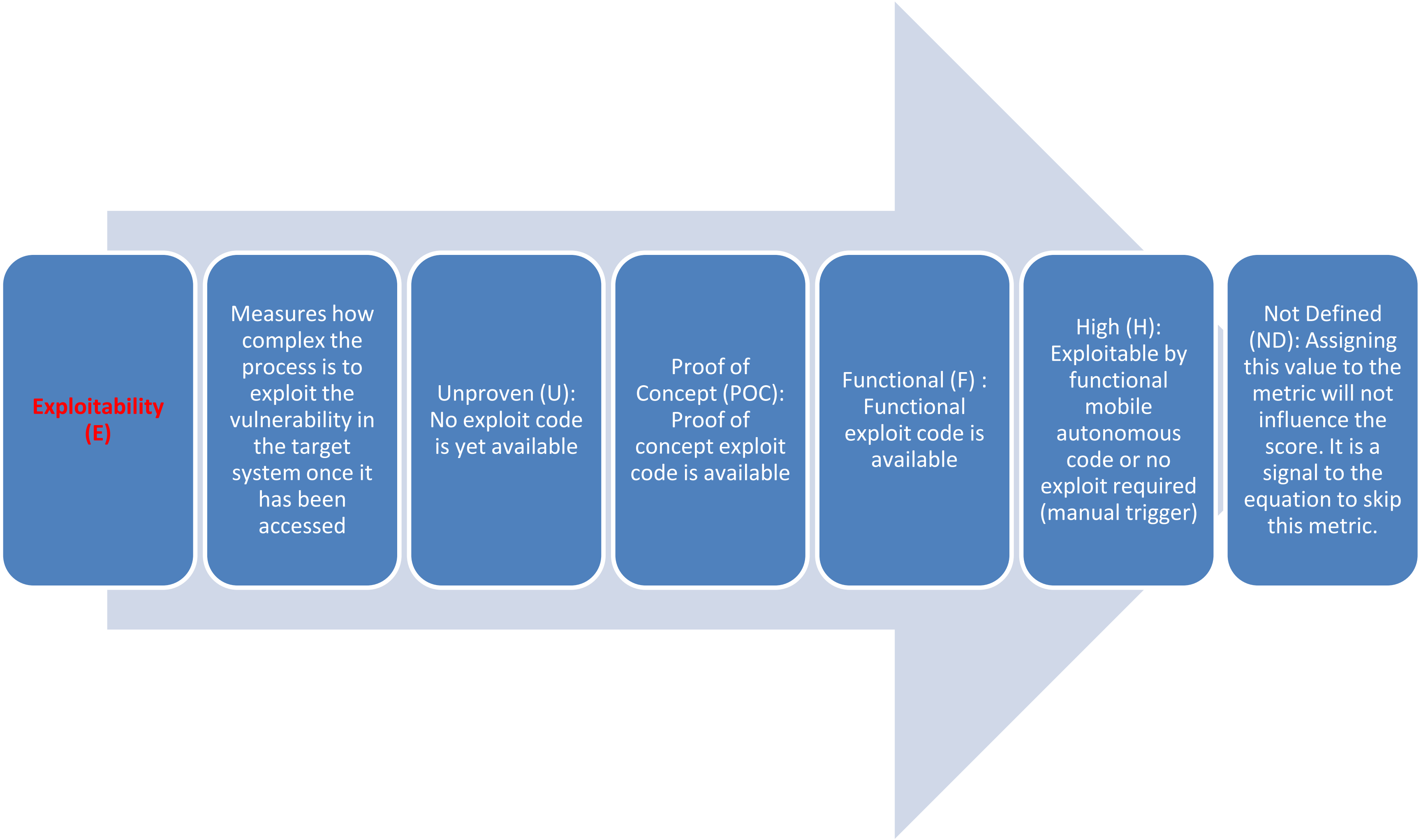
Partial (P) : Considerable lag in or interruptions in resource availability

Complete (C) : Total shutdown of the affected resource

Temporal Metric Group

- Time dependent qualities of a vulnerability
- 3 Temporal metrics

Temporal Metrics



Exploitability (E)

Measures how complex the process is to exploit the vulnerability in the target system once it has been accessed

Unproven (U): No exploit code is yet available

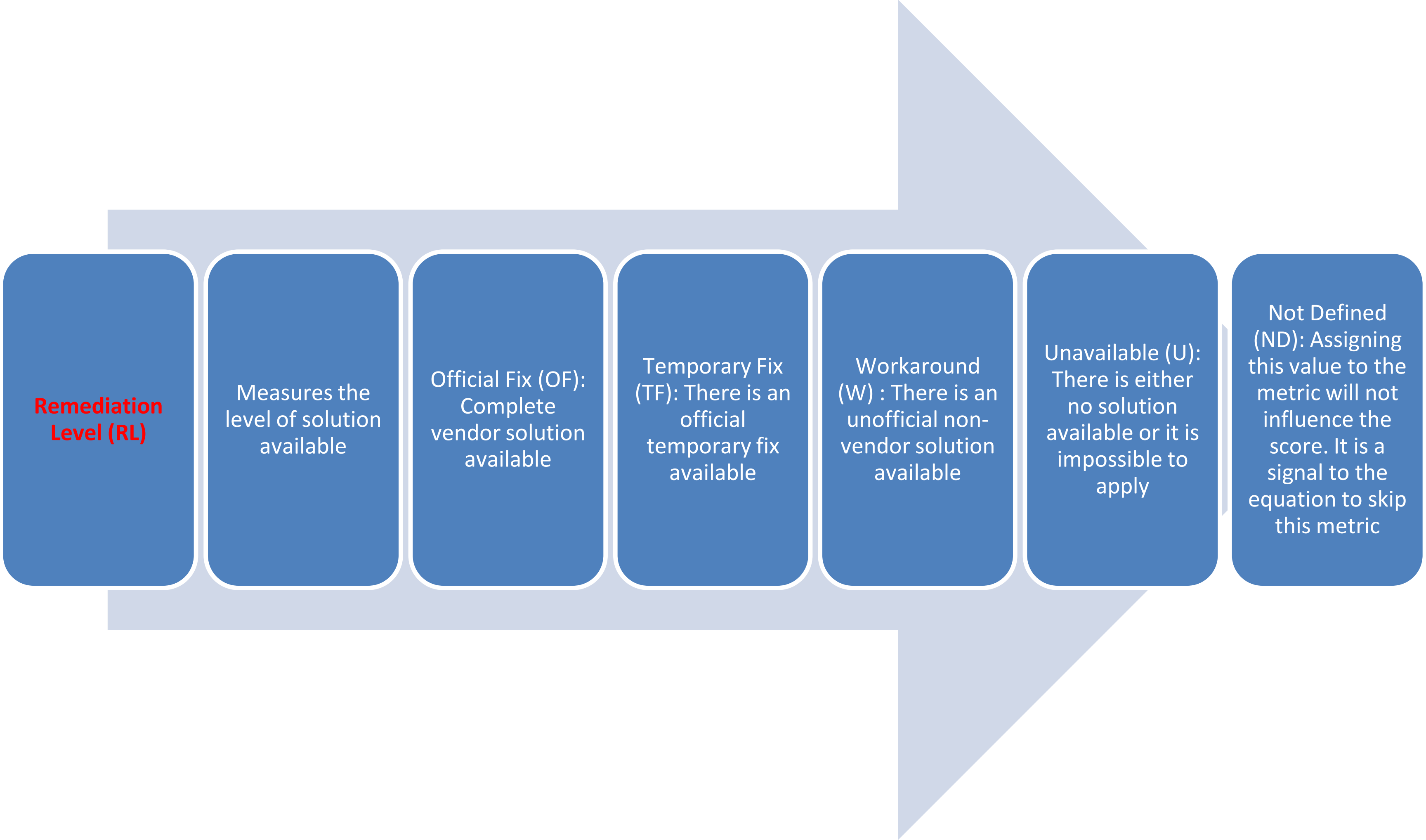
Proof of Concept (POC): Proof of concept exploit code is available

Functional (F) : Functional exploit code is available

High (H): Exploitable by functional mobile autonomous code or no exploit required (manual trigger)

Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Temporal Metrics



Remediation Level (RL)

Measures the level of solution available

Official Fix (OF): Complete vendor solution available

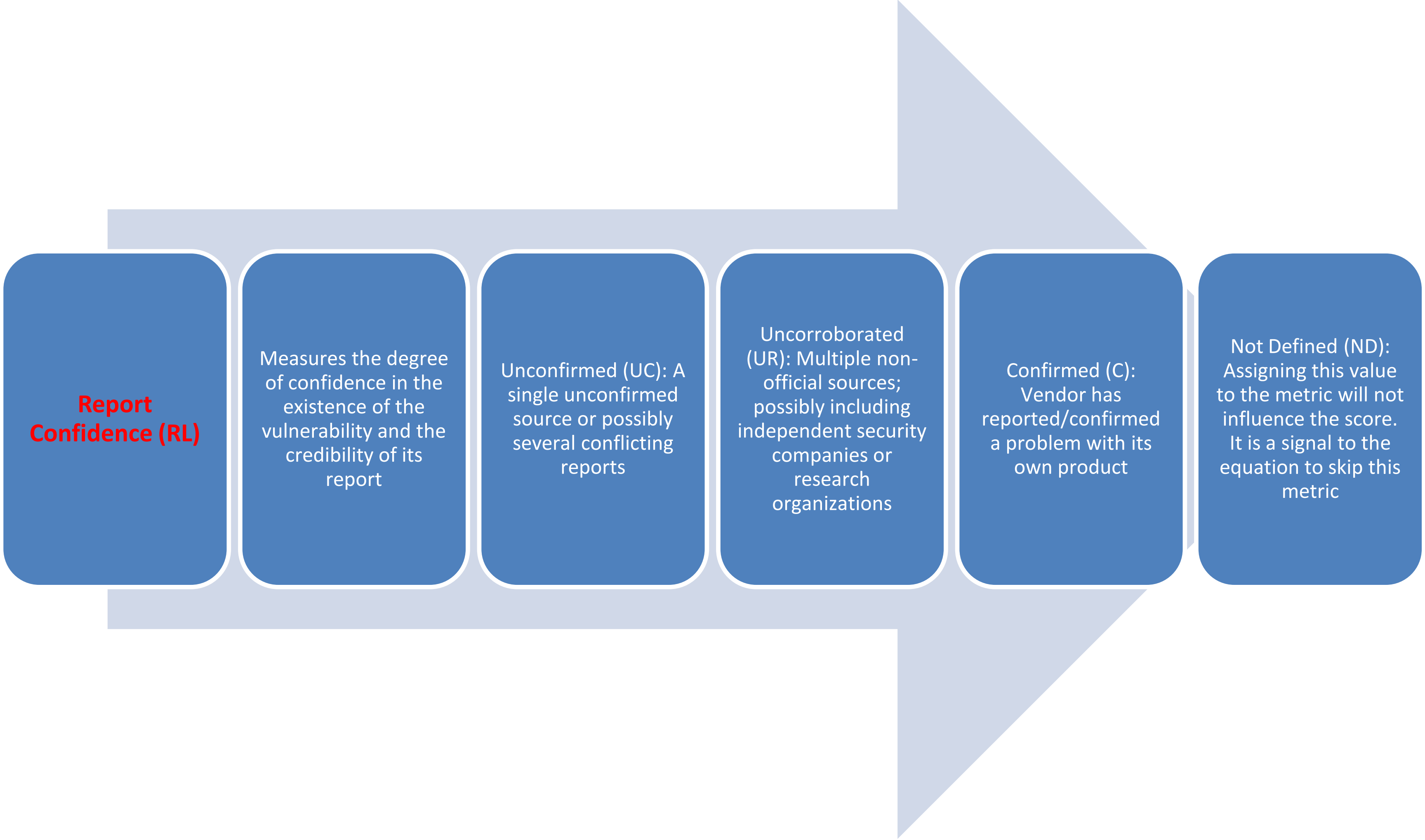
Temporary Fix (TF): There is an official temporary fix available

Workaround (W) : There is an unofficial non-vendor solution available

Unavailable (U): There is either no solution available or it is impossible to apply

Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric

Temporal Metrics



Report Confidence (RL)

Measures the degree of confidence in the existence of the vulnerability and the credibility of its report

Unconfirmed (UC): A single unconfirmed source or possibly several conflicting reports

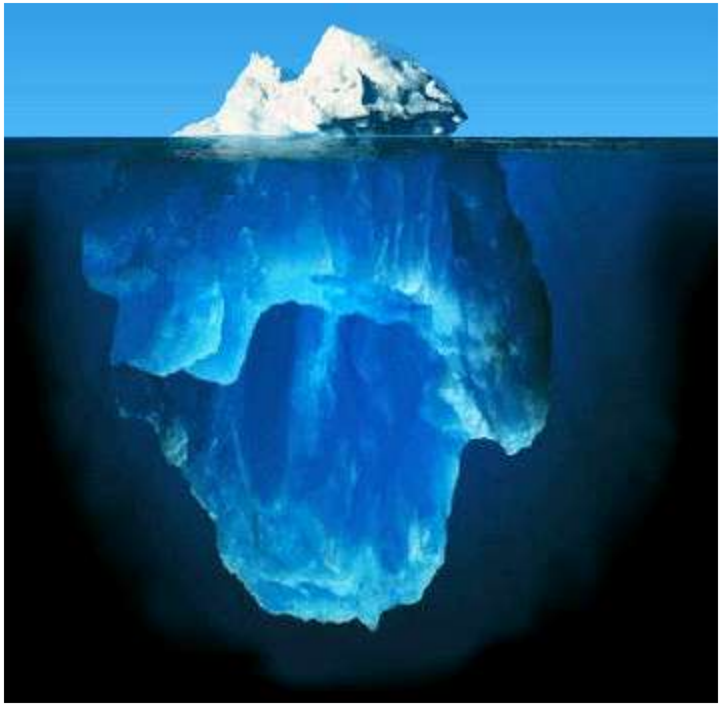
Uncorroborated (UR): Multiple non-official sources; possibly including independent security companies or research organizations

Confirmed (C): Vendor has reported/confirmed a problem with its own product

Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric

Environmental Metric Group

- Implementation and environment specific qualities of a vulnerability
- 3 Environmental metrics



Environmental Metrics

Collateral Damage Potential (CDP)

- This metric measures the potential for loss of life or physical assets through damage or theft of property or equipment.
- None (N): There is no potential for physical assets, productivity or revenue damage
- Low (L): A successful exploit of this vulnerability may result in slight loss of revenue or productivity to the organization
- Low-Medium (LM): A successful exploit of this vulnerability may result in moderate loss of revenue or productivity to the organization.
- Medium-High (MH): A successful exploit of this vulnerability may result in significant loss of revenue or productivity
- High (H):A successful exploit of this vulnerability may result in catastrophic loss of revenue or productivity.
- Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric

Environmental Metrics

Target Distribution (TD)

- Measures the relative size of the field of target systems susceptible to the vulnerability
- None (N) : No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting (0%)
- Low (L): Targets exist inside the environment, but on a small scale (1% - 15%)
- Medium (M): Targets exist inside the environment, but on a medium scale (16% - 49%)
- High (H) : Targets exist inside the environment on a considerable scale (50% - 100%)
- Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric

Environmental Metrics

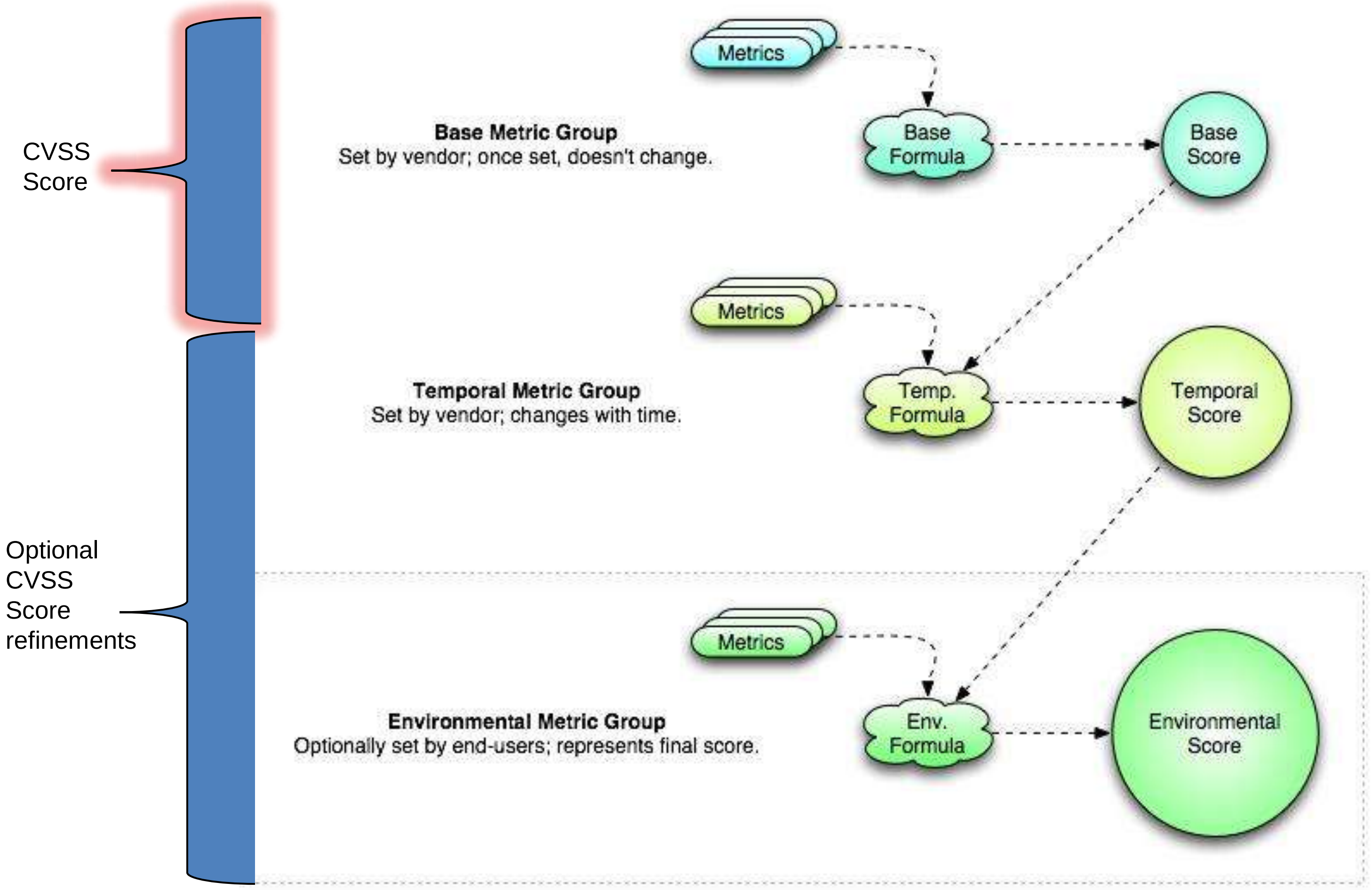
Impact Requirement (IR) based of FIPS 199

- This metric enables the analyst to customize the CVSS score depending on the criticality of the affected IT asset.
- Low (L): Loss of [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization
- Medium (M): Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization
- High (H): Loss of [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization
- Not Defined (ND): Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric

Scoring and Formulas

- The process of combining metric values
- Base score is the “foundation” and stands alone as the CVSS representation of a vulnerability attributes
  - Modified by Temporal and Environmental metrics
- Base and Temporal scores computed by vendors and coordinators with the intent of being published
- Environmental score optionally computed by end-user / organization

CVSS (Scoring View)



Base Metric Group
Set by vendor; once set, doesn't change.

Temporal Metric Group
Set by vendor; changes with time.

Environmental Metric Group
Optionally set by end-users; represents final score.

Base Scoring

- **Computed by vendors and coordinators**
- **Combines innate characteristics of the vulnerability**
- **The base score has the largest bearing on the final score**
  - Computed primarily from the Impact Metrics
- **Represents vulnerability severity**

Temporal Scoring

- Computed by vendors and coordinators
- Modifies the Base Score
- Allows for the introduction of mitigating factors to reduce the score of a vulnerability
- Designed to be re-evaluated at specific intervals as a vulnerability ages
- Represents urgency at specific points in time

Environmental Scoring

- Computed by end users
- Adjusts combined Base-Temporal score
- Should be considered the FINAL score
- Represents a snapshot in time, tailored an environment
- User organizations will use this to prioritize responses within their own environments

Format for publishing Vectors

- Every application or service that uses the Common Vulnerability Scoring System (CVSS) should provide not only the CVSS score - but also a vector describing the components from which the score was calculated.
- This allows end-users to validate score while providing a common set of vulnerability attributes to be disclosed

CVSS Base Vectors

CVSS vectors containing only base metrics take the following form:

(AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C])

http://nvd.nist.gov/cvss.cfm?vectorinfov2

Vector definitions Base

Example 1: (AV:L/AC:H/Au:N/C:N/I:P/A:C)

Example 2: (AV:A/AC:L/Au:M/C:C/I:N/A:P)

Metric: AV = AccessVector (Related exploit range)
Possible Values: L = Local access, A = Adjacent network, N = Network

Metric: AC = AccessComplexity (Required attack complexity)
Possible Values: H = High, M = Medium, L = Low

Metric: Au = Authentication (Level of authentication needed to exploit)
Possible Values: M= Requires multiple instances, S= Requires single instance, N= None required

Metric: C = ConfImpact (Confidentiality impact)
Possible Values: N = None, P = Partial, C = Complete

Metric: I = IntegImpact (Integrity impact)
Possible Values: N = None, P = Partial, C = Complete

Metric: A = AvailImpact (Availability impact)
Possible Values: N = None, P = Partial, C = Complete

Vector definitions Base

Example 1: (AV:L/AC:H/Au:N/C:N/I:P/A:C/E:P/RL:O/RC:C/CDP:L/TD:M/CR:L/IR:L/AR:H)

Example 2: (AV:LN/AC:L/Au:M/C:C/I:N/A:P/E:F/RL:T/RC:UR/CDP:MH/TD:H/CR:M/IR:L/AR:M)

Metric: E = Exploitability (Availability of exploit)

Possible Values: U = Unproven, P = Proof-of-concept, F = Functional, W = Widespread, ND = Not Defined

Metric: RL = RemediationLevel (Type of fix available)

Possible Values: O = Official-fix, T = Temporary-fix, W = Workaround, U = Unavailable, ND = Not Defined

Metric: RC = ReportConfidence (Level of verification that the vulnerability exists)

Possible Values: UC = Unconfirmed, UR = Uncorroborated, C = Confirmed, ND = Not Defined

CVSS Scoring Example (CVE-2002-0392): Apache Chunked-Encoding Memory Corruption

```
--------------------------------------------------------------------------
BASE METRIC              EVALUATION                  SCORE
--------------------------------------------------------------------------
Access Vector                      [Network]          (1.00)
Access Complexity                  [Low]              (0.71)
Authentication                     [None]             (0.704)
Confidentiality Impact             [None]             (0.00)
Integrity Impact                   [None]             (0.00)
Availability Impact                [Complete]          (0.66)
--------------------------------------------------------------------------
BASE FORMULA                    BASE SCORE
--------------------------------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = (0.6*6.9 + 0.4*10.0 – 1.5)*1.176 == (7.8)
---------------------------------------------------------------------------
TEMPORAL METRIC          EVALUATION        SCORE
---------------------------------------------------------------------------
Exploitability                     [Functional]       (0.95)
Remediation Level                  [Official-Fix]     (0.87)
Report Confidence                   [Confirmed]     (1.00)
```

```
--------------------------------------------------------------------------
TEMPORAL FORMULA                 TEMPORAL SCORE
--------------------------------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00) == (6.4)
-----------------------------------------------------------------------------
ENVIRONMENTAL METRIC       EVALUATION        SCORE
-----------------------------------------------------------------------------
Collateral Damage Potential [None - High]  {0 - 0.5}
Target Distribution        [None - High]  {0 - 1.0}
Confidentiality Req.       [Medium]          (1.0)
Integrity Req.           [Medium]          (1.0)
Availability Req.          [High]           (1.51)
------------------------------------------------------------------------------------
ENVIRONMENTAL FORMULA           ENVIRONMENTAL SCORE
------------------------------------------------------------------------------------
AdjustedTemporal == (10*0.95*0.87*1.0) == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1}) == (0.00 - 9.2)
------------------------------------------------------------------------------------
```

CVSS Scoring Example 2 (CVE-2003-0062): NOD32 Antivirus Buffer Overflow

```
---------------------------------------------------------------------------
BASE METRIC             EVALUATION       SCORE
---------------------------------------------------------------------------
                  Access Vector              [Network]
                  (1.0)
Access Complexity         [Medium]                     (0.61)
                  Authentication                          [None]
                  (0.704)
                  Confidentiality Impact       [Complete]
                  (0.66)
                  Integrity Impact             [Complete]
                  (0.66)
                  Availability Impact          [Complete]
                  (0.66)
                  ---------------------------------------------------------------------------
                  FORMULA                              BASE SCORE
                  ---------------------------------------------------------------------------
                  Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
                  Exploitability = 20*0.35*0.704*0.395 == 1.9
                  f(Impact) = 1.176
                  BaseScore =((0.6*10)+(0.4*1.9)–1.5)*1.176 == (6.2)
                  ---------------------------------------------------------------------------
TEMPORAL METRIC          EVALUATION       SCORE
---------------------------------------------------------------------------
Exploitability          [Proof-Of-Concept]             (0.90)
Remediation Level          [Official-Fix]              (0.87)
Report Confidence          [Confirmed]                 (1.00)
```

```
---------------------------------------------------------------------------
FORMULA                        TEMPORAL SCORE
---------------------------------------------------------------------------
round(6.2 * 0.90 * 0.87 * 1.00) == (4.9)
                   ---------------------------------------------------------------------------
-
ENVIRONMENTAL METRIC       EVALUATION        SCORE
---------------------------------------------------------------------------
Collateral Damage Potential [None - High]  {0 - 0.5}
Target Distribution         [None - High]  {0 - 1.0}
Confidentiality Req.        [Medium]          (1.0)
Integrity Req.           [Medium]          (1.0)
Availability Req.         [Medium]          (1.0)
---------------------------------------------------------------------------
FORMULA                      ENVIRONMENTAL SCORE
---------------------------------------------------------------------------
AdjustedTemporal == 4.9
EnvScore = round((4.9+(10-4.9)*{0-0.5})*{0-1}) ==  (0.00 - 7.5)
---------------------------------------------------------------------------
```

application

- **So what does a CVSS Environmental Score of 7.5 for CVE-2003-0062 mean to me?**
  - Your response to 7.5 may be different than mine based on constituency
  - Consistent universal scoring of Base and Temporal categories provides relative severity
  - So far…

0-3	No impact – wait for SP
4-5	Next Patch Cycle
6-7	Within 7 days
7-10	Firedrill

- **Any scoring / normalization of this many variables is going to be a gross generalization**
  - Some subjectivity in evaluating metrics
  - Formulas encode pre-defined values
  - Some things are missed

applications

The Common Vulnerability Scoring System (CVSS) and Its Applicability to US Federal Agency Systems

- NIST IR 7435 is published as final. CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. This publication defines and describes the CVSS standard, provides advice on performing scoring, and discusses how Federal agencies can incorporate Federal Information Processing Standards (FIPS) 199 impact ratings into their CVSS scores to generate scores that are specifically tailored to particular Federal agency environments.
- For complete article see:
- http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf

applications

CVSS and the Payment Card Industry (PCI)

- In order for private-sector firms to process credit cards, they need to comply with the Payment Card Industry Data Security Standards (PCI DSS). Effective June 2007, the PCI governing body is requiring firms use CVSS in order to determine how vulnerable are their IT systems. The PCI DSS is available:
- https://www.pcisecuritystandards.org/pdfs/pci_dss_technical_and_operational_requirements_for_approved_scanning_vendors_ASVs_v1-1.pdf

applications

- Generally, to be considered compliant, a component must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0

The following exceptions or clarifications apply:

- A component must be considered non-compliant if the installed SSL version is limited to Version 2.0, or older. SSL must be a more recent version than 2.0.
- Vulnerabilities or mis-configurations that may lead to DoS should not be taken into consideration

Final comments

- **The authors recognize that many other metrics could have been included in CVSS. We also realize that no one scoring system will fit everyone's needs perfectly.**
- **The particular metrics used in CVSS were identified as the best compromise between completeness, ease-of-use and accuracy. They represent the cumulative experience of the CVSS Special Interest Group members as well as extensive testing of real-world vulnerabilities in end-user environments.**
- **As CVSS matures, these metrics may expand or adjust, making the scoring even more accurate, flexible and representative of modern vulnerabilities and their risks.**

CVSS Usage in NVD

- **NVD receives feeds from CVE**
- **NVD analysts assign CVSS scores (Base only)**
- **Simplified ratings:**
  - High: 7.0 through 10.0
  - Medium: 4.0 through 6.9
  - Low: < 4.0
- **Incomplete information → assume worst case**
  - No details at all = 10.0
- **Early CVE entries use estimated CVSSv2 scores**
- **CVSS calculator available**

http://nvd.nist.gov/cvss.cfm

Important Considerations for CVSS

- **Focuses on impact to the system/box/device**
  - Environmental factors allow some adjustment
  - Full database compromise typically scores at most a 7.0 out of 10.0
- **One CVE can cover multiple issues**
  - Highest score wins
- **Scoring is not 100% repeatable**
  - Dependency on available details
  - Common/default configurations
- **Environmental and temporal scores are under-utilized**

Contact

- Steve Christey coley@mitre.org, cve@mitre.org
  - Tell us how you use CVE!

Questions?