The Common Vulnerability Scoring System (CVSS)

Agenda

- Introduction and overview of CVSS
- Why CVSS?
- Internals
- Scoring
- Industry adoption and call for action
- Closing comments and questions

Overview

CVSS

- 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
- Open
- Usable, understandable, and dissectible by anyone

FIRST™ Improving Security Together

A joint NIAC effort

- Cisco
- Symantec
- Qualys
- eBay
- DHS/MITRE
- CERT/CC
- Microsoft
- ISS

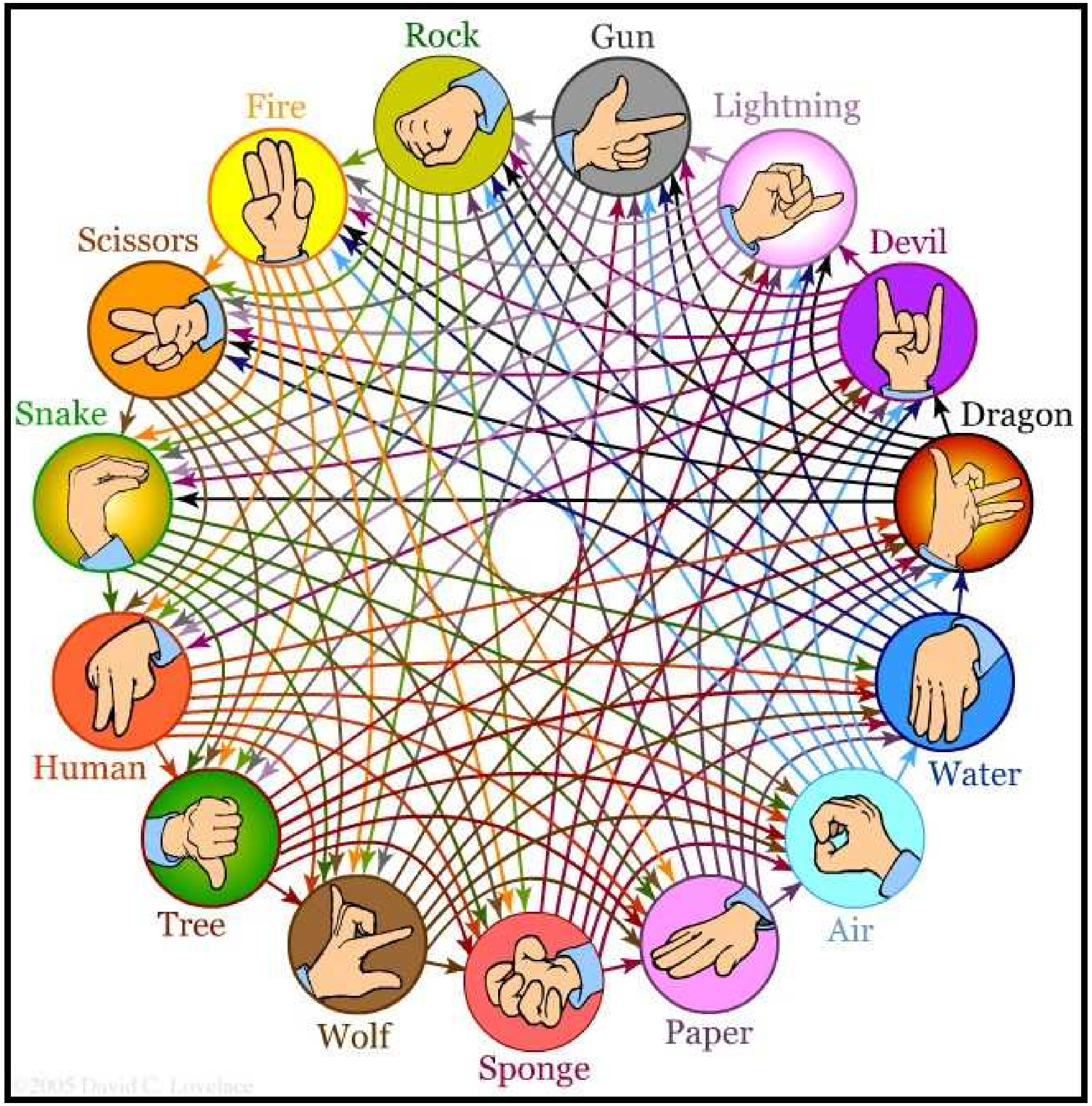
Scope Constraints

- CVSS is not:
  - Threat scoring system (The DHS color warning system)
  - Vulnerability database (Symantec's bugtraq)
  - Real-time attack scoring system (Symantec's ARIS)

Why CVSS?

- Different Organizations
  - Vendors (response)
  - Coordinators (notification, coordination)
  - Reporters (research, discovery)
  - Users (mitigation)
- All have different roles, motivations, priorities, resources, etc
- We need a common way to communicate!

How do we score now?



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, US-CERT

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

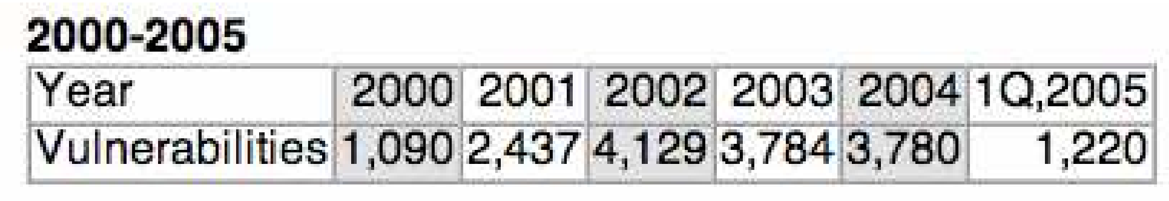
Rating	Definition
Extremely Critical	Typically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild.
Highly Critical	As Above, no known exploits
Moderately Critical	As Above, 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

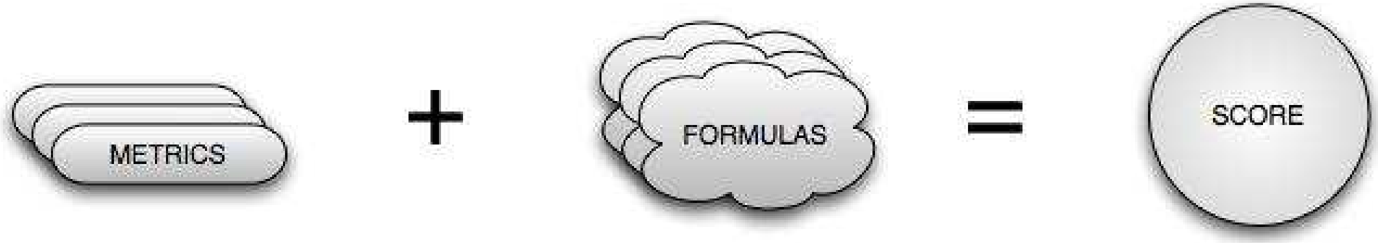
Year	2000	2001	2002	2003	2004	1Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	1,220

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?

How does CVSS work?

- Metrics and formulas yield a score
- That’s all!

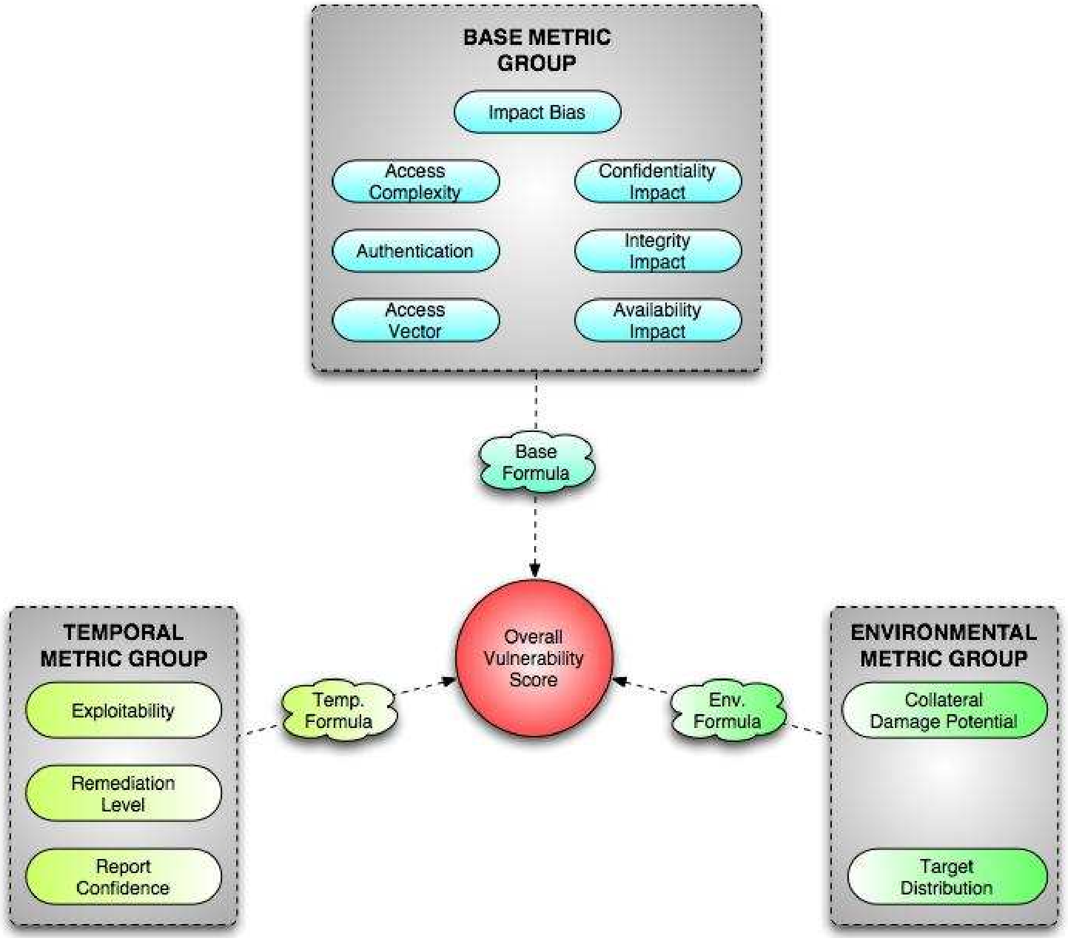


Metrics

- A constituent component or characteristic of a vulnerability that can be quantitatively or qualitatively measured
- Make up the bulk of CVSS
- Three distinct groups
  - Base Metrics
  - Temporal Metrics
  - Environmental Metrics
- Designed with OBJECTIVITY in mind

Improving Security Together

CVSS (Metrics View)



Base Metric Group

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

Base Metrics: Access Vector

- Measures whether a vulnerability is exploitable locally or remotely
- Local: The vulnerability is only exploitable locally
- Remote: The vulnerability is exploitable remotely (and possibly locally as well)

Base Metrics: Access Complexity

- Measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system
- High: Specialized access conditions exist
  - specific windows of time (a race condition)
  - specific circumstances (non-default configurations)
  - victim interaction (tainted e-mail attachment)
- Low: Specialized access conditions or extenuating circumstances do not exist
  - always exploitable (most common case)

Base Metrics: Authentication

- Measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability
- Required: Authentication is required to access and exploit the vulnerability
- Not Required: Authentication is not required to access or exploit the vulnerability

Base Metrics: Confidentiality Impact

- Measures the impact on confidentiality of a successful exploit of the vulnerability on the target system
- None: No impact on confidentiality
- Partial: There is considerable informational disclosure
- Complete: A total compromise of critical system information

Base Metrics: Integrity Impact

- Measures the impact on Integrity of a successful exploit of the vulnerability on the target system
- None: No impact on integrity
- Partial: Considerable breach in integrity
- Complete: A total compromise of system integrity

Base Metrics: Availability Impact

- Measures the impact on Availability of a successful exploit of the vulnerability on the target system
- None: No impact on availability
- Partial: Considerable lag in or interruptions in resource availability
- Complete: Total shutdown of the affected resource

Improving Security Together

Base Metrics: Impact Bias

- Allows a score to convey greater weighting to one of three impact metrics over the other two
- Normal: Confidentiality Impact, Integrity Impact, and Availability Impact are all assigned the same weight
- Confidentiality: Confidentiality impact is assigned greater weight than Integrity Impact or Availability Impact
- Integrity: Integrity Impact is assigned greater weight than Confidentiality Impact or Availability Impact
- Availability: Availability Impact is assigned greater weight than Confidentiality Impact or Integrity Impact.

Temporal Metric Group

- Time dependent qualities of a vulnerability
- 3 Temporal metrics

Temporal Metrics: Exploitability

- Measures how complex the process is to exploit the vulnerability in the target system once it has been accessed
- Unproven: No exploit code is yet available
- Proof of Concept: Proof of concept exploit code is available
- Functional: Functional exploit code is available
- High: Exploitable by functional mobile autonomous code or no exploit required (manual trigger)

Temporal Metrics: Remediation Level

CVSS

- Measures the level of solution available
- Official Fix: Complete vendor solution available
- Temporary Fix: There is an official temporary fix available
- Workaround: There is an unofficial non-vendor solution available
- Unavailable: There is either no solution available or it is impossible to apply

FIRST™ Improving Security Together

Temporal Metrics: Report Confidence

- Measures the degree of confidence in the existence of the vulnerability and the credibility of its report
- Unconfirmed: A single unconfirmed source or possibly several conflicting reports
- Uncorroborated: Multiple non-official sources; possibly including independent security companies or research organizations
- Confirmed: Vendor has reported/confirmed a problem with its own product

Environmental Metric Group

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

Environmental Metrics: Collateral Damage Potential

- Measures the potential for a loss in physical equipment, property damage or loss of life or limb
- None: There is no potential for property damage.
- Low: A successful exploit of this vulnerability may result in light property damage or loss
- Medium: A successful exploit of this vulnerability may result in significant property damage or loss
- High: A successful exploit of this vulnerability may result in catastrophic property damage and loss

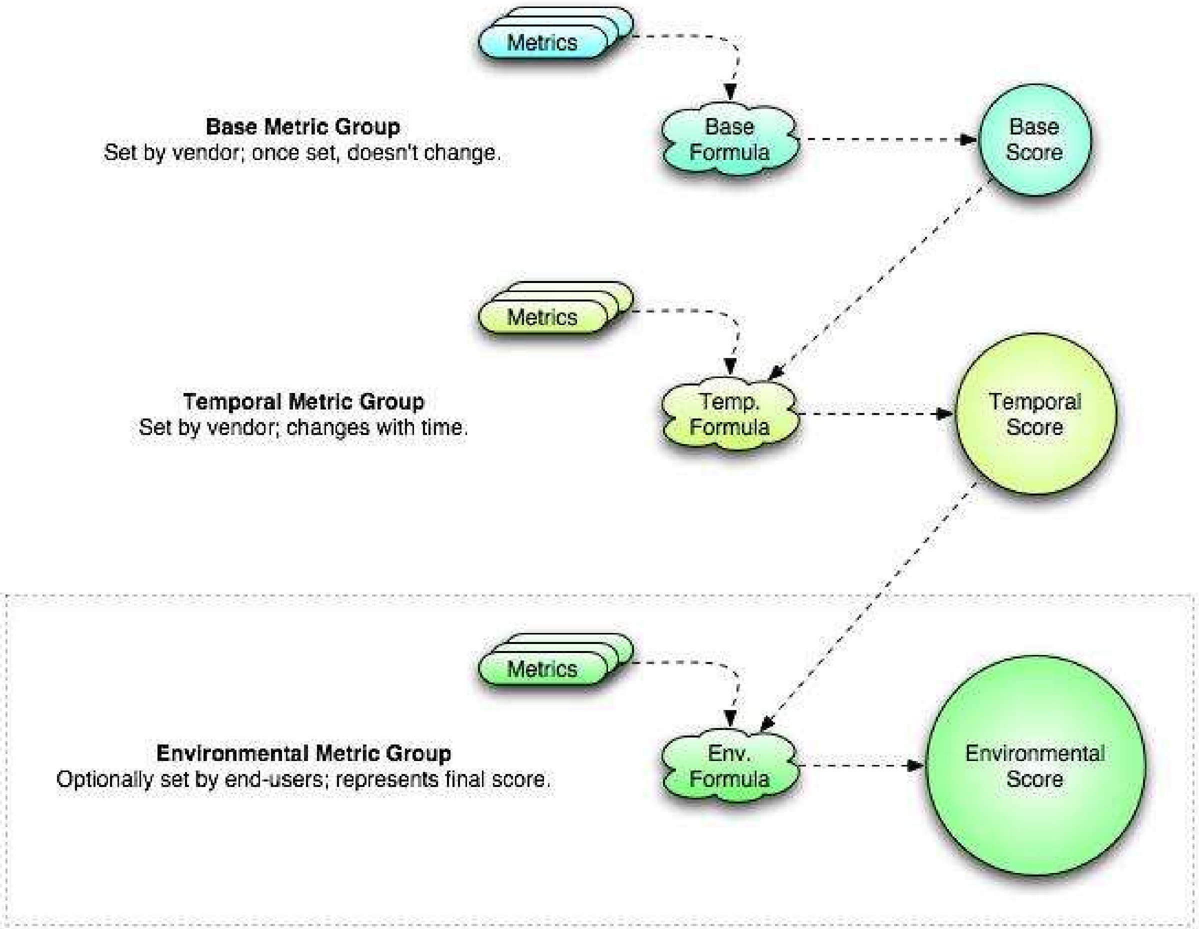
Environmental Metrics: Target Distribution

- Measures the relative size of the field of target systems susceptible to the vulnerability
- None: No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting (0%)
- Low: Targets exist inside the environment, but on a small scale (1% - 15%)
- Medium: Targets exist inside the environment, but on a medium scale (16% - 49%)
- High: Targets exist inside the environment on a considerable scale (50% - 100%)

Scoring and Formulas

- The process of combining metric values
- Base score is the “foundation”
  - 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)


Metrics
Base Metric Group
Set by vendor; once set, doesn't change.
Base Formula
Base Score
Metrics
Temporal Metric Group
Set by vendor; changes with time.
Temp. Formula
Temporal Score
Metrics
Environmental Metric Group
Optionally set by end-users; represents final score.
Env. Formula
Environmental 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

Base Scoring Formula

```
BaseScore = round to 1 digit of 10
* (case AccessVector          of local:    0.7   remote:       1.0)
* (case AccessComplexity      of high:     0.8   low:          1.0)
* (case Authentication        of required: 0.6   not-required: 1.0)
* ((case ConfidentialityImpact of none:    0     partial:      0.7  complete: 1.0)
*  (case ImpactBias           of normal:   0.333 CNFDNTLTY:    0.5  INTGRTY:  0.25 AVLBLTY:  0.25)
+  (case IntegrityImpact      of none:     0     partial:      0.7  complete: 1.0)
*  (case ImpactBias           of normal:   0.333 CNFDNTLTY:    0.25 INTGRTY : 0.5  AVLBLTY : 0.25)
+  (case AvailabilityImpact   of none:     0     partial:      0.7  complete: 1.0)
*  (case ImpactBias           of normal:   0.333 CNFDNTLTY:    0.25 INTGRTY : 0.25 AVLBLTY : 0.5))
```

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

Temporal Scoring Formula

```
TemporalScore = round to 1 digit of BaseScore
 * (case Exploitability  of unproven:    0.85 proof-of-concept: 0.9 functional: 0.95 high: 1.00)
 * (case RemediationLevel of official-fix: 0.87 temporary-fix:   0.90 workaround: 0.95 unavail: 1.00)
 * (case ReportConfidence of unconfirmed:  0.90 uncorroborated:  0.95 confirmed:  1.00)
```

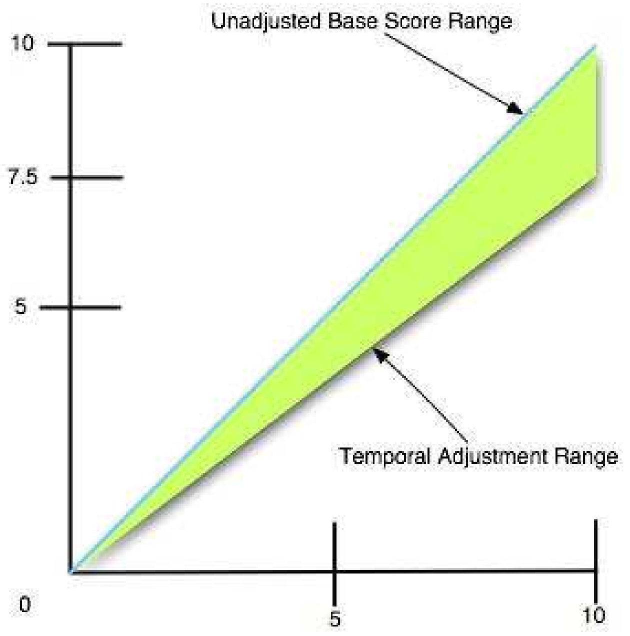
Environmental Scoring

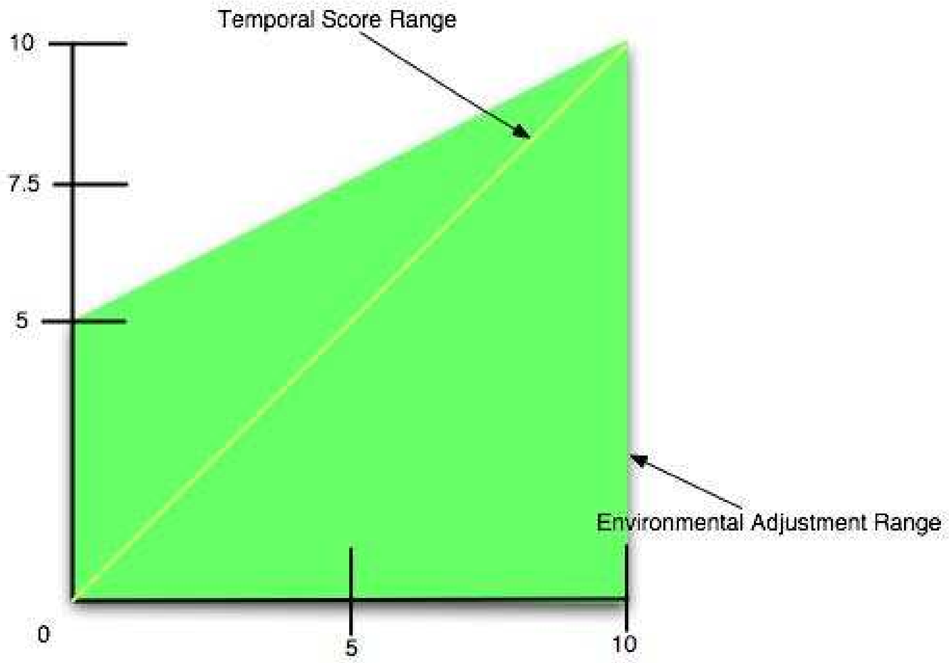
- Computed by end users
- Adjusts combined Base-Temporal score
- Should be considered the FINAL score
- Represents a snapshot in time, tailored an environment
- User organizations will use this to prioritize responses within their own environments

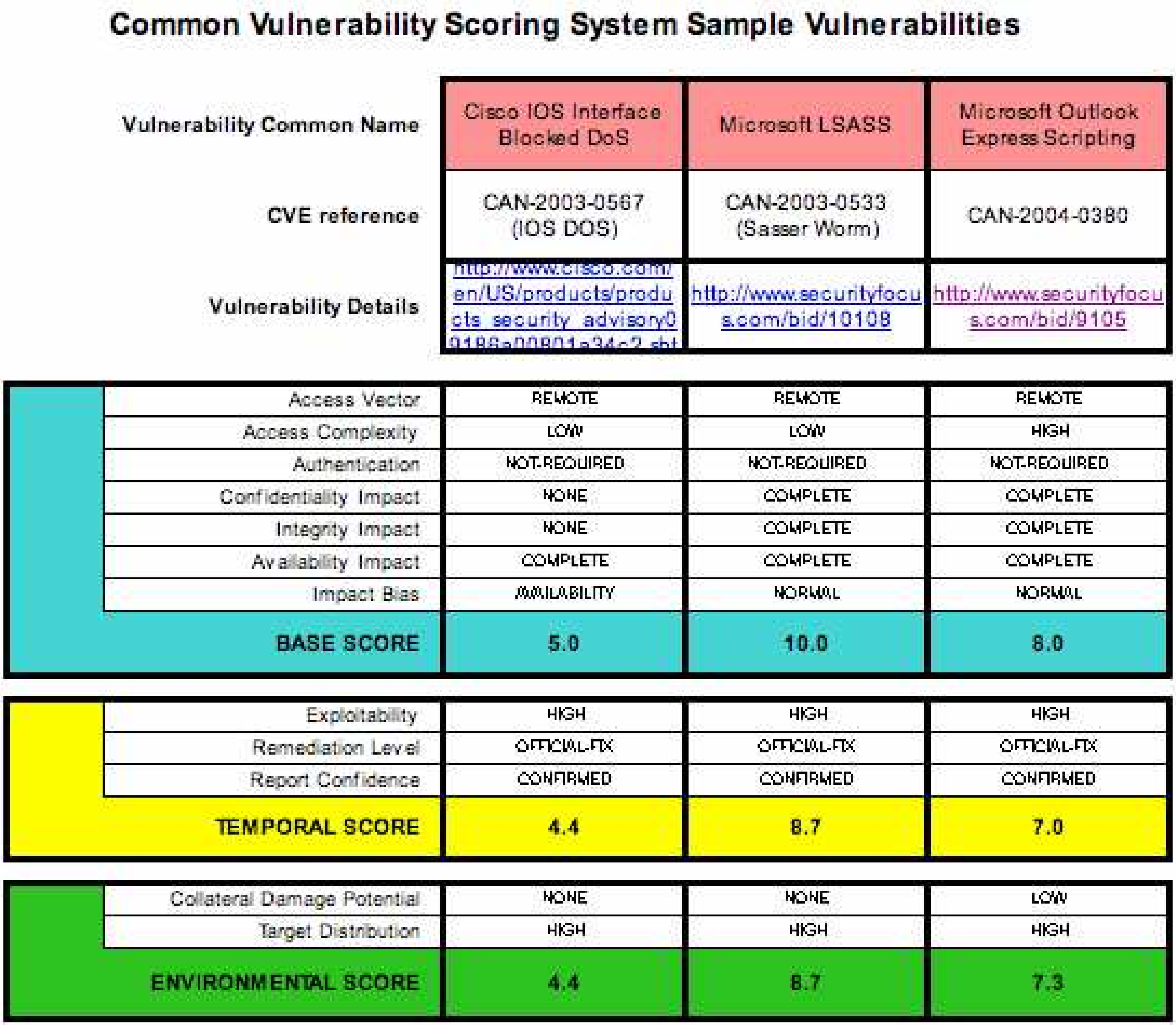
Environmental Scoring Formula

```
EnvironmentalScore = round to 1 digit of (TemporalScore + (10 - TemporalScore)
* (case CollateralDamagePotential of none: 0 low: 0.1  medium: 0.3  high: 0.5))
* (case TargetDistribution      of none: 0 low: 0.25 medium: 0.75 high: 1.00)
```

Temporal and Environmental Scoring Ranges







Common Vulnerability Scoring System Sample Vulnerabilities

Vulnerability Common Name	Cisco IOS Interface Blocked DoS	Microsoft LSASS	Microsoft Outlook Express Scripting
CVE reference	CAN-2003-0567 (IOS DOS)	CAN-2003-0533 (Sasser Worm)	CAN-2004-0380
Vulnerability Details	http://www.cisco.com/en/US/products/products_security_advisory09186a00801a34c2.sht	http://www.securityfocus.com/bid/10108	http://www.securityfocus.com/bid/9105
Access Vector	REMOTE	REMOTE	REMOTE
Access Complexity	LOW	LOW	HIGH
Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED
Confidentiality Impact	NONE	COMPLETE	COMPLETE
Integrity Impact	NONE	COMPLETE	COMPLETE
Availability Impact	COMPLETE	COMPLETE	COMPLETE
Impact Bias	AVAILABILITY	NORMAL	NORMAL
BASE SCORE	**5.0**	**10.0**	**8.0**
Exploitability	HIGH	HIGH	HIGH
Remediation Level	OFFICIAL-FIX	OFFICIAL-FIX	OFFICIAL-FIX
Report Confidence	CONFIRMED	CONFIRMED	CONFIRMED
TEMPORAL SCORE	**4.4**	**8.7**	**7.0**
Collateral Damage Potential	NONE	NONE	LOW
Target Distribution	HIGH	HIGH	HIGH
ENVIRONMENTAL SCORE	**4.4**	**8.7**	**7.3**

Industry Adoption

Organization	Status	Organization	Status
Akamai	Adopted	npower	Evaluating
Amazon	Evaluating	RWE	Evaluating
American Water	Adopted	Symantec	Rolling out
ArcSight	Evaluating	Qualys	Rolling out
Cisco	Adopted	Tenable	Rolling out
eBay	Evaluating	Thames Water	Adopted
IBM	Evaluating	Union Pacific	Adopted
McAfee	Evaluating	webMethods	Rolling out
netForensics	Evaluating	CSC	Evaluating

CVSS Example

- Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows (**CAN-2005-1983**)

- **Description: Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm.**

CVSS Example (base)

- Buffer overflow in the Plug and Play (PnP) service for Microsoft Windows

Access Vector	REMOTE
Access Complexity	LOW
Authentication	NOT-REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	NORMAL
BASE SCORE	**10.0**

CVSS Example (temporal)

- Buffer overflow in the Plug and Play (PnP) service for Microsoft Windows

Exploitability	HIGH
Remediation Level	OFFICIAL-FIX
Report Confidence	CONFIRMED
TEMPORAL SCORE	**7.8**

CVSS Example (enviromental)

Collateral Damage Potential	HIGH
Target Distribution	MEDIUM
ENVIRONMENTAL SCORE	**7.0**

Metric Usage

- **So what does a CVSS Environmental Score of 7.0 for CAN-2004-0380 mean to me?**
  - We have a SIG to get that data from CVSS evaluators
  - Your response to 8.6 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 some pre-defined values
  - Some things are missed

Call for action

- CVSS needs you!

- How you can help:
  - Adoption
  - Join the SiG
    - Financial Services needs representation in the CVSS SiG

Where to find CVSS examples on the web

- FIRST: http://www.first.org/cvss
- NIST: http://nvd.nist.gov/cvss.cfm?showall and http://nvd.nist.gov/cvss.cfm?calculator.
- Cisco MySDN: http://tools.cisco.com/MySDN/Intelligence/home.x
- Nessus: http://www.nessus.org/plugins/index.php?view=newest

Roadmap

- Monthly SiG meetings
- Evangelism
  - Continued industry adoption
- Improvements and add-ons

Summary

- CVSS is a way to talk about vulnerability severity
- New
- Open
- Simple
- Objective
- Comprehensive