The Common Vulnerability Scoring System

Mike Schiffman, Cisco Systems

The RSA Conference, February 2005

Today’s Agenda

- Introduction and overview of CVSS
- A bit of Background and some Scope constraints
- What are Metrics?
- How is Scoring done?
- What’s Next for CVSS?
- Closing comments and Questions

Introduction and Overview

- Common Vulnerability Scoring System (CVSS)
- National Infrastructure Advisory Council (NIAC) tasked in support of the global Vulnerability Disclosure Framework
  - Solves problem of multiple, incompatible scoring systems in use today
- A universal language to convey vulnerability severity and help determine urgency and priority of response
- Open
- Usable and understandable by anyone

Joint Effort

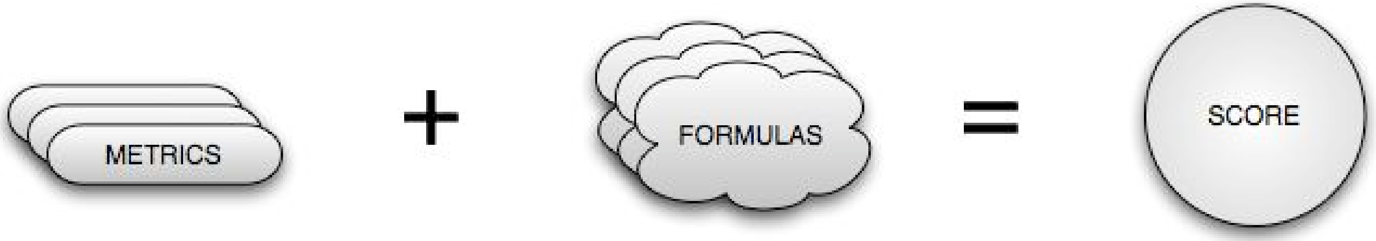
- Many contributors
  - Cisco
  - Symantec
  - Qualys
  - eBay
  - DHS/MITRE
  - CERT/CC
  - Microsoft
  - ISS

Scope Constraints

- What CVSS isn't:
  - Threat scoring system (DHS color warning system)
  - Vulnerability database (bugtraq)
  - Real-time attack scoring system (Symantec's ARIS)

What's under the hood?

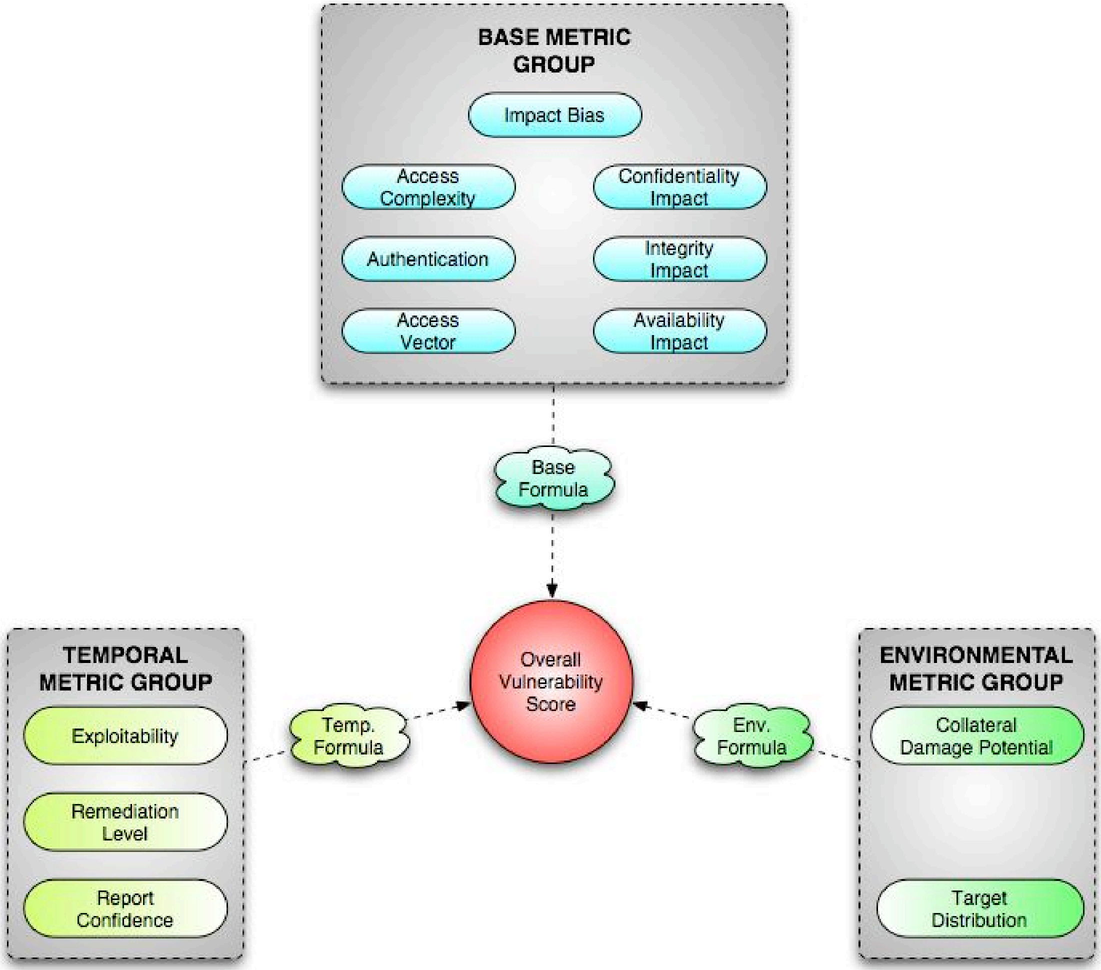
- Metrics and Formulas
- That's all!



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

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

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

- 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

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

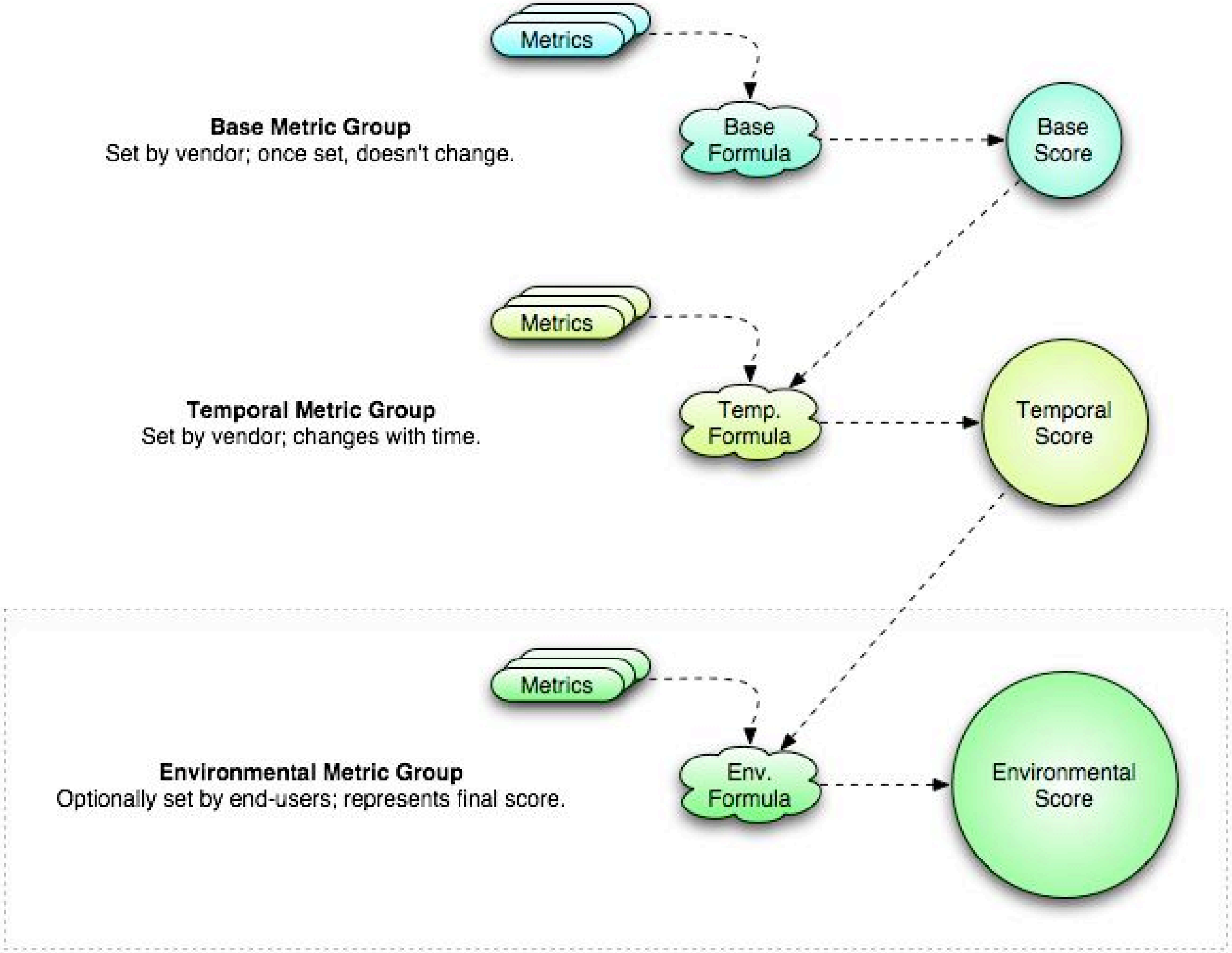
Environmental Metrics: Target Distribution

- 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 Formula
Base Score
Base Metric Group
Set by vendor; once set, doesn't change.
Metrics
Temp. Formula
Temporal Score
Temporal Metric Group
Set by vendor; changes with time.
Metrics
Env. Formula
Environmental Score
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***

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 confirme
1.00)
```

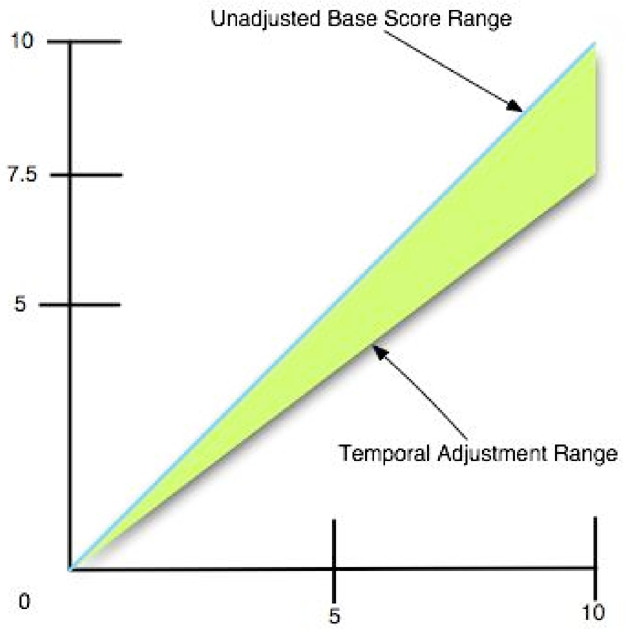
Environmental Scoring

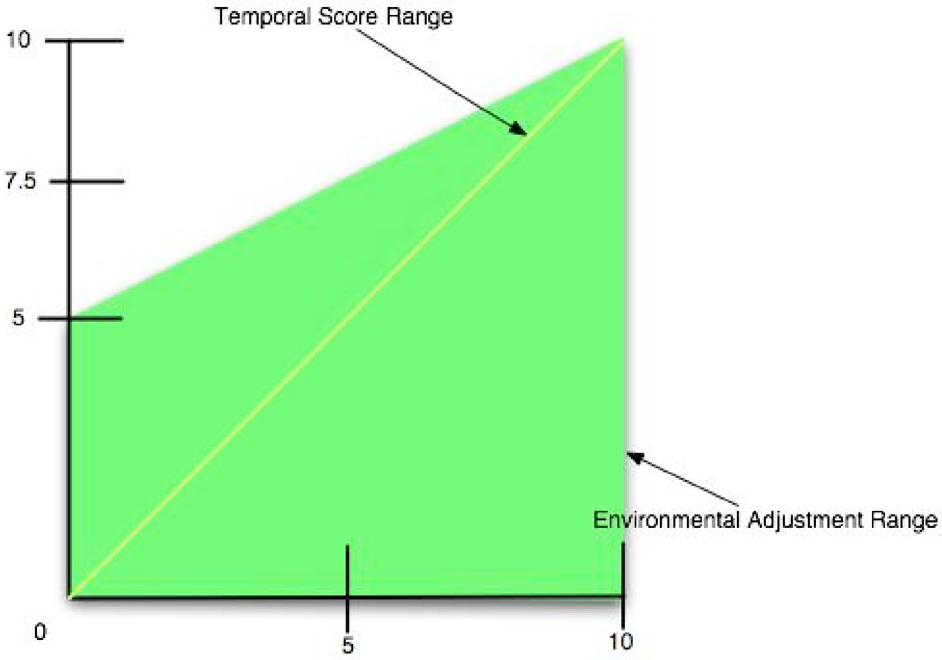
- Computed by end users
- Adjusts combined Base-Temporal score
- Should be considered the FINAL score
- Represents a snapshot in time, tailored an environment
- User organizations will use this to ***prioritize responses*** within their own environments

Environmental Scoring Formula

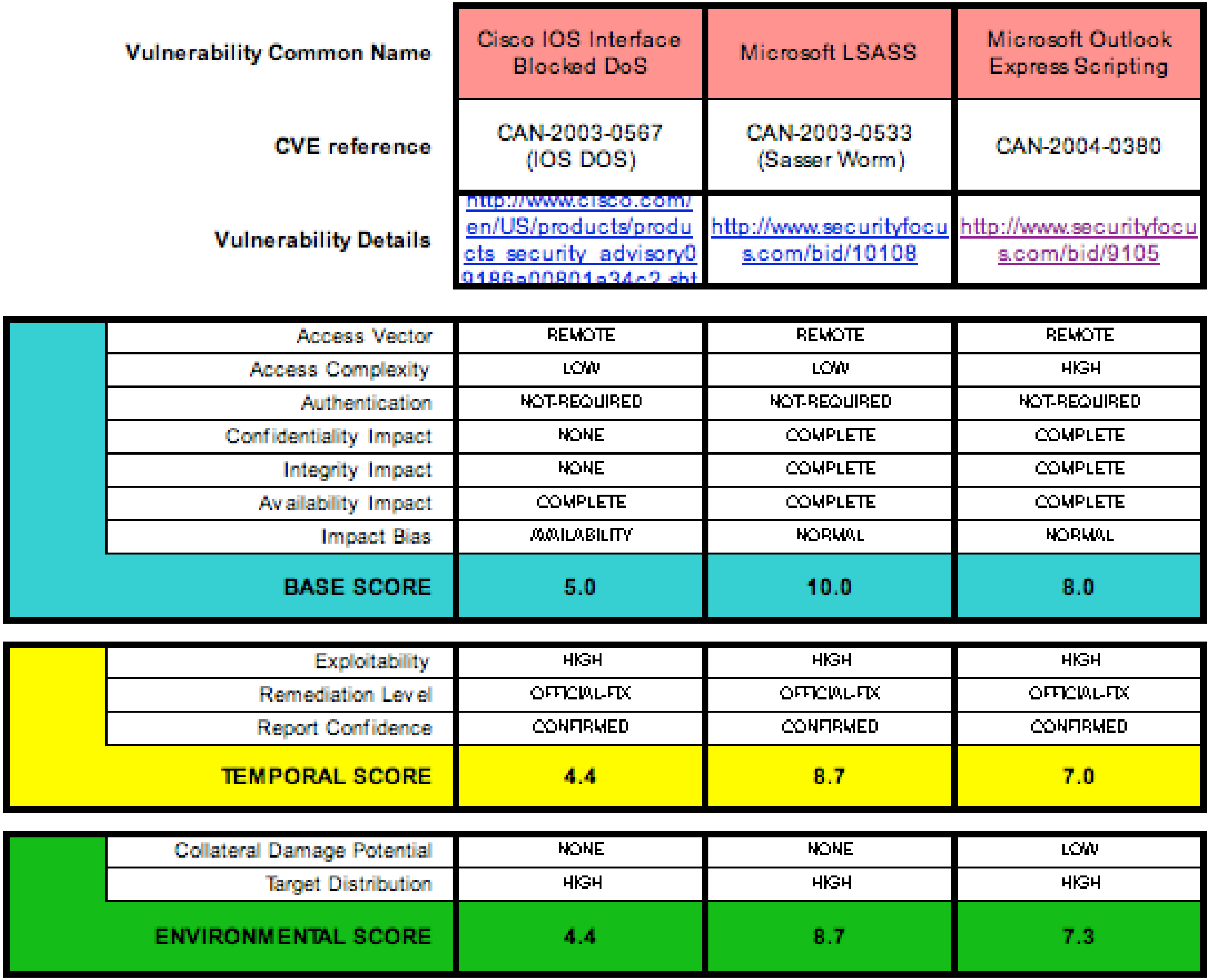
```
EnvironmentalScore = round to 1 digit of (TemporalScore + (10 -
TemporalScore)
* (case CollateralDamagePotential of none: 0 low: 0.1  medium: 0.3  high:
0.5))
* (case TargetDistribution        of none: 0 low: 0.25 medium: 0.75 high:
1.00)
```

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

Roadmap

- NIAC submitted to President January 2005
- DHS, CVSS developers encouraging widespread, voluntary adoption
- Several NIAC member companies have adopted
  - Union Pacific
  - American Water
  - Symantec
  - Akamai
- Others are adopting in some form
  - CERT/CC
  - US-CERT
  - Qualys
  - Cisco
- Seeking permanent home
- IETF Draft being written

Frequently Asked Questions (1 of 5)

- Q: I am an end-user (CISO/CSO/operations security guy), is there anything I need to do?

- A: Typically, application and security product vendors will provide both the BASE and TEMPORAL scores to you. As the end user, you need only calculate your ENVIRONMENTAL score.

Frequently Asked Questions (2 of 5)

- Q: I am an application or product security vendor, why should I use CVSS and publish CVSS temporal scores?

- A: As more vendors begin publishing CVSS scores, more customers will understand and appreciate the advantages. They will grow to appreciate the ability to tailor scores to their environment and begin to look for, and expect CVSS scores of all their suppliers. Consider PGP’s web of trust and eBay’s feedback network. The more it is used, the better it works.

Frequently Asked Questions (3 of 5)

- Q: I am an end-user, and really like the {VENDOR_NAME} scoring method, why should I change to CVSS?

- A: Other systems are closed competing standards, do not offer a mutable scoring framework, and do not consider different environments.

Frequently Asked Questions (4 of 5)

- Q: Ok tough-guy, what does CVSS really offer that other scoring methodologies don't?

- A: An open framework that can be used, understood, and improved upon by anybody to score vulnerabilities. It a nutshell, *it's just plain better*.

Frequently Asked Questions (5 of 5)

- Q: CVSS Sounds great! Give me the code!
- A: Well, we don't have code. CVSS is a framework that you can use to develop an application suitable to your needs, your environment or your customers. Our team put together an XLS document for testing purposes.

Summary

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

Conclusion

- Comments and questions
- How can you help? Urge your vendor to support CVSS scoring!
- Feel free to email me: Mike Schiffman (mschiffm@cisco.com)