

CVSS

The Common Vulnerability Scoring System

June 2004
NIAC Vulnerability Disclosure Working Group
Scoring Subgroup

John Chambers
President & CEO
Cisco Systems, Inc.

John Thompson
Chairman & CEO
Symantec Corp.

Agenda

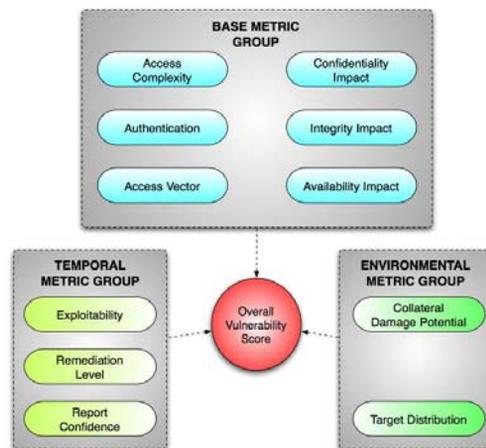
- Status
- CVSS update
 - Changes to the model
 - Scoring process
 - Formulae
- Next steps
- Timeline

June 2004 Status

- ❑ 90% complete
 - System designed, metrics, formulae, scoring methodology completed
 - Completed formulas and scoring
 - ❑ Engaging industry for testing
 - Phase one
 - ❑ In-house testing by designers
 - Phase two
 - ❑ Tapping other industry for participation
 - ❑ Commitment from Qualys and Symantec to implement the final version of CVSS
-

3

The CVSS



Base Metric Group Scoring

- Has the largest bearing on the final score
 - Provides the foundation for the final score
- The impact metrics have the strongest weight on the base score
 - Confidentiality
 - Integrity
 - Availability

Temporal Metric Group Scoring

- Can modify the base score by 0 to 25% downwards from the initial value
- Allows for the introduction of mitigating factors to reduce the threat score of a vulnerability
- Designed to be re-evaluated at specific intervals as a vulnerability ages

Environmental Metric Group Scoring

- Potentially decreases or increases the final score
- Environmental metric group allows for organizations to adjust the severity of a vulnerability within on the context of their own environment

Next Steps

- Testing:
 - Stress tests: dry run system through several selected vulnerabilities
 - Validate with industry study groups
- Take feedback from testing and improve system
- Complete report to NIAC
- Pending NIAC review, implement CVSS (TBD: [html/asp/xml/Excel](#))
- Pending NIAC approval and industry acceptance, submit IETF draft

Timeline

- ❑ August 01, 2004: complete real world testing
- ❑ August 30, 2004: complete feedback and finalize CVSS
- ❑ September 15, 2004: complete report for NIAC

Three Examples

Vulnerability	Microsoft Outlook Express scripting vulnerability	Microsoft LSASS vulnerability	BGP route flapping denial of service vulnerability
Typical Exploit	W32/Netsky.B virus	Sasser worm	None known

Access Vector	REMOTE	REMOTE	REMOTE
Access Complexity	HIGH	LOW	HIGH
Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED
Confidentiality Impact	COMPLETE	COMPLETE	NONE
Integrity Impact	COMPLETE	COMPLETE	NONE
Availability Impact	COMPLETE	COMPLETE	COMPLETE
BASE SCORE	8.3	10.0	2.8

Exploitability	FUNCTIONAL	HIGH	PROOF-OF-CONCEPT
Remediation Level	OFFICIAL-FIX	OFFICIAL-FIX	TEMPORARY-FIX
Report Confidence	CONFIRMED	CONFIRMED	CONFIRMED
TEMPORAL SCORE	7.2	9.1	2.3

Collateral Damage Potential	NONE	NONE	NONE
Target Distribution	HIGH	HIGH	HIGH
ENVIRONMENTAL SCORE	7.2	9.1	2.3

Discussion

Questions?
