Minutes for the CVSS SIG meeting – 06/20/2006 Meeting:
This meeting was held on Tuesday, June 20, 2006
Conference Call

Attending: George Theall, Seth Hanford, Karen Kent, Luann Johnson, Sasha Romanosky, Mike Scheck, Art Manion, Stav Raviv, Robin Sterzer

Agenda/Discussion:

1) Report status on action items from previous meeting on, 04/18/06:
   a. Gavin/Mike – Document PSIRT team's findings and issued discovered into the best practice documentation – In Progress. Gavin has added items to the document, but Mike is unsure if it has been sent for comments.
   b. Peter – Write up on the CVSS algorithm findings (after voting complete) – Will need to follow up with Peter
   c. Gavin – Seek out vendors to adopt CVSS – No Updates
   d. Gavin – Provide dates/times for BoF at Baltimore – Mike will work on with those attending the conference to determine if there is any time and date to have a BoF
   e. Team – Vote on Change proposal #1 – Impact Bias Metric; Change proposal #2 – Additional documentation on CIA metric; Change proposal #3 – Reword Access Complexity definition – Done
   f. Team – Comment and provide feedback on Change proposal #4 – Additional granularity on Target Distribution and Change proposal #5 – Additional granularity for Access Vector – Done. We will be discussing them below in item 3)
2) CVSS Structure, Strategy and Process:
   a. Methodology for incorporating feedback into CVSS – N/A
   b. Comparison on CVSS Scores
      i. Discuss the results from the vendor scoring – Karen provided information on the NIST and Cisco vendor scoring discussion. Analyst from both companies went through four or five set of vulnerability comparisons. Each analyst went through the vulnerabilities posted and discussed them. They found that there were some discrepancies and common problems. Some assumptions that the analyst made will be discussed in the proposals.
3) Administrative:
   a. CVSS v1.x documentation status update and proposed changes – Details for each proposal will follow after notes taken and actions taken from the meeting in italics for your review.
      i. Proposal #4: Additional Granularity for Target Distribution (Release Date: 4/12/06; revised 4/24/06; Status: Not yet voted on) – Numbers appear to be high especially for large enterprise. Art will work on the percentages and qualify the numbers. The idea is to have these as guidelines and recommendations to help the in determining what are best for ones environment.
      Decision: Everyone agreed that we are better off with more granularities and the principle. More work to be done on the proposal and send for voting. Art will work on it and resubmit
      Add an additional option for the target distribution network as defined below. End users need an additional level of granularity for assigning the target distribution metric.

      This metric measures the number of target systems susceptible to the vulnerability. It is meant as an environment-specific indicator in order to approximate the percentage of systems within the environment that could be affected by the vulnerability. This reflects the observation that after a "critical mass" of vulnerable systems is reached, it becomes less important to record different levels of granularity. In other words, the difference between 65% and

95% is not as important as the difference between 45% and 25%. These ranges should be treated as guidelines. The scorer can modify the ranges to best fit the environment.

Scoring Evaluation
Guidelines for scoring the target distribution metric are as follows:

None: No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. As best as can be determined, no systems currently deployed within the environment depend on target systems for business operations. Effectively 0% of the environment is considered at risk.

Low: Targets exist inside the environment, but on a small scale. Between 1% – 15% of the total environment is considered at risk.

Low-Medium: Targets exist inside the environment, but on a medium scale. Between 16% – 39% of the total environment is considered at risk.

Medium-High: Between 40% – 59% of the total environment is considered at risk.

High: Targets exist inside the environment on a considerable scale. Between 60% – 100% of the total environment is considered at risk.

ii. Proposal #5: Additional Granularity for Access Vector (Release Date: 4/12/06 (revised 4/24/06; Status: Not yet voted on) – Feedback received from others is that this is a good idea but need to clearly define what local is. We need to include more examples and clarification
Decision: Mike will work on additional qualification to be added to the proposal on what local is and then it can be sent out for voting.

Add a new option to the access vector metric for vulnerabilities that are accessible only over a local network. The option would be called "Local network accessible" (sometimes referred to as "adjacent" in the CVSS SIG email list discussions). See below for a detailed definition.

Vulnerabilities that can be exploited from adjacent locations have the the same requirements as remote except that the source of the attack is restricted to a logically or physically nearby location. For example, a vulnerability that can only be exploited from the same subnetwork or ethernet segment is considered adjacent. Also, a vulnerability that requires physical proximity, such as 802.11 or bluetooth radio range, is also considered adjacent.

A vulnerability that is adjacently exploitable will have a higher score than a locally exploitable vulnerability and a lower score than a remotely exploitable vulnerability.

iii. Proposal #6: Modification to Collateral Damage Potential (Release Date: 4/25/06; Status: Not yet voted on) – Team agreed on the proposal but need to define what electronic means
Decision: Sasha will update the document with what electronic means; pass it around with the team for feedback. Once feedback received the proposal can be up for voting.

The existing collateral damage potential metric measures only potential "physical or property" damage. However, this definition leaves out the possibility of non-physical electronic damage which is by far the most common type of damage we

see with computer vulnerabilities. Thus, we need to modify the metric so that it covers both physical and non-physical damage.

iv. Proposal #7: Modification of Access Vector and Authentication Metrics (Release Date: 4/25/06; Status: Not yet voted on) – The idea is good, but adds a layer of complexity. Luann is concern that the person doing the scoring would need to know the ins and outs of the vulnerability. This might sacrifice accuracy for usability. Art strongly recommends separating the access from authentication. If unsure of the vulnerability err on being overly cautious.
This requires multiple authentications. How complex is the vulnerability to exploit is a way to simplify the user.
Decision: Change the authentication metrics to low, medium and high. Seth will work on the revision and send out to the team.

The existing access vector metric includes elements of authentication (e.g. "local" requires that you authenticate to the OS or else have physical access to the computer). This is confusing to users of the standard because we have a separate authentication metric. Therefore, we propose to remove all elements of authentication from the access vector metric and the move those elements to the existing authentication metric.

Access Vector Metric:
1. Network accessible (i.e., the vulnerable software accepts packet information from the network stack)
2. Non-network accessible (i.e., the vulnerable software does not accept packet information from the network stack)
3. Requires physical access

Note: this proposal doesn't include a fourth possible option for the access vector, "Local network accessible/Adjacent", because this option will be voted on in proposal #5.

Authentication Metric:
1. Requires no authentication
2. Requires application authentication (but not OS authentication)
3. Requires OS authentication (but not application authentication)
4. Requires OS and application authentication

Note: the authentication metric measures what level of authentication/authorization is needed prior to launching the attack. The exact type of authentication is not being measured (e.g., we don't care for this metric whether or not an application authenticates using OS credentials or its own private scheme).

v. Proposal #8: Direct and Indirect Impact of Exploitation (Release Date: 6/16/06; Status: Not yet voted on) – Mike agrees with the feedback that was provided on the list that this one is not ready to be voted on. Measuring the weakness the system might have
Decision: Mike will work on this one further.

Our multi-organization scoring comparison effort has revealed that the scoring of vulnerabilities that potentially have an impact on secondary hosts that access exploited servers, such as cross site scripting (XSS) vulnerabilities, is the cause of a large source of CVSS scoring discrepancies between multiple IT security organizations. For example, some analysts score XSS vulnerabilities with respect

to the direct impact on the server, and some score them with respect to the indirect impact on an end user of the server.

In order to make scoring consistent and to focus scoring on the software that is directly vulnerable, the CVSS documentation should be updated to reflect that vulnerabilities should always be scored with respect to the impact on the vulnerable server.

Note: This proposal is an expansion of the original Proposal #8, which was focused solely on XSS vulnerabilities. The original proposal took this approach based on the conclusions surrounding a discussion during the last CVSS SIG conference call. However, we need to clearly define our arguments for making this decision prior to voting on this proposal. As suggested by Sasha, we will consider adding an environmental metric to capture the indirect impact of exploitation, but that will not be done as part of this proposal.

vi. Proposal #9: Assumptions for Application Privileges (Release Date: 6/16/06; Status: Not yet voted on)
Decision: This proposal requires further discussion on the list. Sasha will begin the discussion. Once additional feedback is received we will need to update the proposal and discuss is it ready for voting.

Our multi-organization scoring comparison effort has revealed that a major source of scoring discrepancies is different assumptions made by analysts as to the privileges under which various applications, such as Web servers and Web browsers, are run. For example, the scores for exploiting a Web server will be quite different if the Web server is assumed to run with root-level or user-level privileges.

To make scoring more consistent, the CVSS documentation should be updated to indicate that vulnerabilities should be scored based on the privileges that are most often used for the application. This does not necessarily reflect the best practice for the application, especially for client applications, which are often run with root-level privileges. If it is not clear what privileges are most often used for an application, analysts should assume the default configuration.

Note: The privilege assumptions were previously discussed on the CVSS SIG list, and while the consensus was that assuming the most often used privileges was the best method, there was also concern that this would lead to scoring inconsistencies. We may want to discuss ideas for addressing those inconsistencies before voting on this proposal.

vii. Proposal #10: Handling Multiple Exploitation Methods (Release Date: 6/16/06; Status: Not yet voted on) – Score off the worse possible scenario.
Decision: Proposal needs to be updated with the exact changes and sent out to the team for voting.

Our multi-organization scoring comparison effort has revealed that some scoring discrepancies are due to analysts taking different approaches to handling cases where there is more than one way to exploit a particular vulnerability. For example, a vulnerability could be exploited using a low-complexity method to gain user-level access, and exploited using a high-complexity method to gain root access.

To make scoring more consistent, the CVSS documentation should be updated to indicate that analysts should generate a score for each approach to exploitation and then assign the vulnerability the highest of the scores. If the highest score is shared by multiple approaches, then analysts should compare those approaches and select the one that is most likely to be used.

Note: To the best of our knowledge, this topic has not yet been discussed on the CVSS SIG mailing list. The alternative approach to this proposal is to have analysts decide which exploitation method is most likely to be used and generate a score just for it.

4) Roundtable: Updates/Needs/Questions

Action Items:

1) Gavin/Mike – Document PSIRT team's findings and issued discovered into the best practice documentation
2) Peter – Write up on the CVSS algorithm findings (after voting complete)
3) Gavin – Seek out vendors to adopt CVSS
4) Mike – Work with those going to the FIRST conference in Baltimore to schedule dates/times for BoF
5) Art – Work on Proposal #4 and send to team
6) Mike – Work on Proposal #5 and 8 and send to team
7) Sasha – Work on Proposal #6 and 9 and send to team
8) Seth – Work on Proposal #7 and send to team
9) Team – Start further discussion on Proposal #10