Minutes for the CVSS PRE-SIG meeting – 07/08/2005 Meeting:
This meeting was held on Friday, July 8, 2005
Conference Call

Attending: Troy Bollinger, Dave Dobrotka, Gerhard Eschelbeck, Barrie Brook, Gavin Reid, Luann Johnson, Anton Chuvakin, Sasha Romanosky, Art Manion, Peter Allor, Yurie Ito, Robin Sterzer

Agenda:

1) Roll call
2) Report status on action items from previous meeting on, 05/19/2005:
   a. Mike – Set up the mailers
   b. Mike – research archiving the mailers
   c. Robin – Schedule next meeting
   d. Catherine – Work with Mike Scheck on the development of the scoring documentation.
   e. Robin – Provide to the team the link to Security Intel
   f. Gavin send the intro email on SIG to FIRST
3) CVSS Structure, Strategy and Process:
   a. Discuss who should own the CVSS version 2 documentation
   b. Discuss who should own the Scoring Best Practices documentation
4) Administrative:
   a. Go over the discussion at FIRST BOF
   b. Set schedule for testing
5) Roundtable: Updates/Needs/Questions

Discussions:

1) Roll call
2) Report status on action items from previous meeting on, 05/19/2005:
   a. Mike – Set up the mailers - Done
   b. Mike – research archiving the mailers – Mike and Don are looking into archiving the mailers
   c. Robin – Schedule next meeting – Done. Future meetings will be on Thursday's at 7:00 (pst)
   d. Catherine – Work with Mike Scheck on the development of the scoring documentation
   e. Robin – Provide to the team the link to Security Intel – Done
   f. Gavin send the intro email on SIG to FIRST – Done
3) CVSS Structure, Strategy and Process:
   a. Discuss who should own the CVSS version 2 documentation – The SIG group owns the document, contents and verification. Need to assign a person to own the gathering of the data for the document. This person would have the list of the data available to be discussed at team meetings.
      - Gavin proposes that Mike Shiffman to take on this role. There are no objections.
      - Roadmap for version 2 will have list of changes, comments, and discrepancies. A six month freeze to do scoring. From this will determine what to be published in version 2
   b. Discuss who should own the Scoring Best Practices documentation – We are missing general best practices for the scoring. This best practice should include what the scores mean. Catherine Nelson has volunteered to own this document. No objections. Anton has volunteered to help out Catherine on this.
      - Pete – Include best practices learned by quarter
      - Gerhard – content to the scoring

- Barrie – sensitivity of the variables need to be looked at
- Pete – Have the availability to provide comments to other on what we have and said
- Gavin – Define how to interact with us on this process and post it to the web (action item)

4) Administrative:
   a. Go over the discussion at FIRST BOF – Team had a good discussion at Singapore. Gavin will send out the meeting notes to the team (action item)
   b. Set schedule for testing – Below are different methods for testing:
      i. Groups score vulnerability specifically interested in and publish to the CVSS team. See if scoring meets.
      ii. Take 4 to 5 vulnerabilities a week and send them to the team to all score
      iii. Go back a year of old vulnerabilities and score together.
      iv. Go back and pick a random 100 vulnerabilities and score. The team will discuss their findings.
      - Luann – focus on the same vulnerabilities to discuss
      - Art – propose random samples and score the same thing. 100 or under
      - Pete – couple that are straight forward to get an understanding of the baseline upfront
      - Team agrees on starting off small and run through the group. Once familiar with the process expand the scope to include more vulnerabilities. Will start off with 4 to 5 vulnerabilities a week then expand.
      - Concern – 1 to 10 is meaningless. Vendor numbers will not be enough to know what the numbers means. Third document "Best Practices for Vendors" to publish their scores. This should be added to our best practices document. This document to include steps on how they got there; numbers (scoring) means different things to different group. Mike S. is looking into this and if there are any overlaps
      - Sasha – Confidentiality and integrity would be thought differently per an organization. Its no reason why it would be scored differently. Military would think it as a higher priority. This would be reflected in the environment category.
      - Base score should not be changed. This will need to be explained.
      - Will also need to explain why it is important to publish the steps of setting a score

5) Roundtable: Updates/Needs/Questions

Troy – Need to be added on the cvss-sig list (action item)

Dave – No comments

Gerhard – No comments

Barrie – No comments

Luann – New to the team. Can find the FIRST documentation at first.org/cvss

Anton – Question on initial emails, where should they go, core group or sig list? SIG group is responsible for CVSS Version 2 and involved in it more such as score vulnerabilities. This is not an open mailer

Sasha – Need to add to the list. He will send new email address to Gavin.(action item)

Some ideas – spreadsheet to log data and a link to post. Will we be publishing scores on the FIRST site? This will be up to the vendors to do it or other groups. Discussions with Application vendors on scoring are still too early to start in our process. We will do this but slowly and build a body of knowledge.

Sharing the scores – all vendors collaborate on this. Pete will take this up with Gerhard and Anton. They are in agreement to figure this out. It will take several months to plan it out, conduct research and obtain feedback. They will publish scores from those different areas. (Action item)

Art – Owes Gavin slides from FIRST and will send to the list (action item). Have a way to sample vulnerabilities and will send out to the team by using the CERT database to get the information (action item).

Pete – Question on communications via the list or website to download from. Team will work together on the list. Website will be used to publish things such as minutes, documentation, etc that are on a high level.

Action Items:

1) Mike – research archiving the mailers – Mike and Don are looking into archiving the mailers
2) Catherine – Work with Mike Scheck on the development of the scoring documentation
3) Mike – Own CVSS Version 2 documentation
4) Catherine/Anton – Own Best Practices documentation
5) Gavin – Define how to interact with us on this process and post it to the web
6) Gavin – Send meeting minutes from Singapore
7) Mike/Gavin – Add Troy to mailers and add Sasha's new address
8) Pete/Anton/Gerhard – Collaborate on sharing the scores within vendors.
9) Art – Send slides from FIRST to team and Gavin
10) Art – Provide vulnerability samples to the team