Minutes of the CVSS PRE-SIG meeting –05/19/2005 Meeting:
This meeting was held on Thursday, May 19, 2005 at 7:00 (pst)
Conference Call

Attending: Gavin Reid, Mike Schiffman, Gerhard Eschelbeck, Dave Proulx, Mike Caudill, Yurie Ito, Catherine Nelson, Art Manion, Steve Christey, Robin Sterzer

Agenda:

1) Rollcall
2) Report status on action items from previous meetings, if any:
3) CVSS Structure, Strategy and Process:
   a. What the membership of the SIG should look like (Constituency, needs, numbers, etc.)
   b. What is expected from the SIG members
   c. Changes to CVSS - suggest we freeze the current CVSS for a period of x months so we can try it and get a good feeling for strengths and weakness. Is it needed to do a one time pre-freeze changes?
4) Administrative:
5) Roundtable: Updates/Needs/Questions

Discussion:

1) Rollcall
2) Report status on action items from previous meetings, if any: None
3) CVSS Structure, Strategy and Process:
   a. What should the membership of the SIG should look like (Constituency, needs, numbers, etc.)
   - Would like to send details of what the SIG looks like; such as, Special Interest Group members we want in the CVSS in the introductory email to first.
   - CVSS scoring has some overhead we want people who have the job of scoring vulnerabilities as his/her job description. Have them report back on their findings and how it is working
   - FIRST people can invite non-first constituents if they are the right fit (for example a CSIRT member might invite the patching point of contact.
   - Group size that is workable 20 preferable to a max 40 people with non-participants dropped after 6 months.
   - Area type for the members and the minimum and maximum amount:
     i. Vendors with vulnerability research groups that would be score vulnerabilities. – 2 to 6
     ii. Large Enterprise (different functions such as Financial and Medical) – 5 to 10
     iii. Existing scoring systems operators – 2 to 4
     iv. NON-CERT Government people with patching and threat management responsibilities – 2-4
     v. University (who do these responsibilities) – 2 to 4
     vi. CERT – 2 to 4
     vii. Admin/Doc (Meeting organizer, Website, Changes) – 2
   b. What is expected from the SIG members
   - Attendance and participation
   - Scoring and providing reports on it. Score the vulnerability and report back on what was done based on the score
   - Push this forward – Evangelism of CVSS – Represent CVSS
   - Provide specific additions and changes for version 2
   - Write documents and present
   - SIG and FIRST to create metrics and milestones. Provide the information

c. Changes to CVSS - suggest we freeze the current CVSS for a period of x months so we can try it and get a good feeling for strengths and weakness. Is it needed to do a one time pre-freeze changes?
   - However the documentation does not need to be frozen and can be augmented during this period. .
   - Go forward with CVSS as is – no need for any last minute pre release changes
   - How companies are implementing the portal and how is it scored will take some time to initiate
   - Recommend no changes for 9-12 months. This timeframe is too long; suggest that the freeze be for 3 to 6 months. Team agreed on a 6 month freeze.

4) Administrative:
   - Mailers – need to set them up; one public mailer to provided feedback to the team (cvss-info@first.org) and another one for the SIG core team (cvss-sig@first.org).
   - Mike will set up the mailers and will look into seeing if FIRST has the capability of archiving them
   - On the public mailer look into have auto-responding with basic FAQ information.
   - How often should the team meet? Every 2 to 4 weeks. Team agreed on Monthly.
   - Schedule a date and place to have a face to face meeting with the team. Possibilities are at the quarterly meetings following the TC meeting.
5) Roundtable: Updates/Needs/Questions
   a. Mission Goal – FIRST taking the CVSS to the next level
   b. Test out version 1 of CVSS by the Security Community
   c. Need adoption and fine tuning
   d. Adopt by Vendors for a year or two
   e. To be tracked by the SIG – Categorize and score vulnerabilities and what was done
   f. Gerhard will be presenting on CVSS. He will only discuss what is public. Gerhard will share the documentation with the team.
   g. Catherine suggested having a document written explaining the scoring process. She will work with Mike Scheck on this.
   h. Provide link to the Security Intel that has been developed by Catherine's team http://tools.cisco.com/MySDN/Intelligence/home.x (note need CEC account)

Action Items:

1) Mike – Set up the mailers
2) Mike – research archiving the mailers
3) Robin – Schedule next meeting
4) Catherine – Work with Mike Scheck on the development of the scoring documentation.
5) Robin – Provide to the team the link to Security Intel
6) Gavin send the intro email on SIG to FIRST