

Agenda for the CVSS SIG meeting – 11/16/2005 Meeting:

This meeting was held on Wednesday, November 16, 2005
Conference Call

Attending: Pete Mill, Luann Johnson, Andrew, Mike Caudill, Jerry Bongard, Sasha Romanosky, Barry Brook, Mike Scheck, Gavin Reid, Robin Sterzer

Agenda:

- 1) Roll call
- 2) Report status on action items from previous meeting on, 10/18/2005:
 - a. Gavin. – Make a formal request to have mailer archived
 - b. Catherine/Anton/Mike Scheck – Own Best Practices documentation draft to team prior to next team meeting
 - c. Catherine – Add Mike Scheck to Best Practices documentation meetings
 - d. Pete/Anton/Gerhard – Collaborate on sharing the scores within vendors – They will set up a meeting for next week to discuss this further. – The meeting has not happened. Anton will take this action item. This is specific to vendors.
 - e. Gavin – Send team the verbiage for “levels/type of actions” to be taken by the team for agreement and adoption – Mike and Gavin are working on this. The draft has been sent but did not include CVSS score. They will send the document out when it is completed.
 - f. Mike C. – Provide comments and feedback to the team from his meeting with Microsoft
 - g. Catherine – Confirm that Bryan Banta is available to tabulate the scores. – Bryan has written the front-end to save the scores. There are still some things missing. A meeting will need to be scheduled to gather the requirements. Gavin has someone who can enter the data.
 - h. Gavin – Follow up on date, time and topic for In-person meeting at FIRST TC On November 14-15th in Redwood City, CA – Many are unable to attend in person. Should we have the meeting in person? Gavin will send an email to the mailer to see who can attend
 - i. Mike S. – Have a friend working on a CVSS Logo
- 3) CVSS Structure, Strategy and Process:
 - a. Methodology for incorporating feedback into CVSS
 - b. Scoring:
 - None (just send packets; connect to 80/tcp, etc)
 - Registered (register for forum, authentication to service, no identity verification)
 - Authenticated (intended to have credentials - sysadmin created them)
 - c. Scoring Comparison
 - d. Scoring Examples – Adding additional examples; who do we get to add them in
 - e. Testing (was scheduled to end on November 4th)
- 4) Administrative:
 - a. Status on groups sharing scoring vulnerabilities
 - b. CVSS v1.x documentation status update and proposed changes
 - c. CVSS Logo – Do we adopt?
 - d. National Vulnerability Database CVSS Support
- 5) Roundtable: Updates/Needs/Questions

Discussion:

- 1) Roll call
- 2) Report status on action items from previous meeting on, 10/18/2005:

- a. Gavin. – Make a formal request to have mailer archived – Gavin followed up on the request. Mike C. indicates that the mailing lists are being archived, but do not have a way that they can be searched. He is looking into a way to do this.
 - b. Catherine/Anton/Mike Scheck – Own Best Practices documentation draft to team prior to next team meeting – The document is becoming critical. Gavin recommends we give this action item to someone else. He will send an email out looking for volunteers (action item)
 - c. Catherine – Add Mike Scheck to Best Practices documentation meetings – N/A
 - d. Pete/Anton/Gerhard – Collaborate on sharing the scores within vendors – They will set up a meeting for next week to discuss this further. – The meeting has not happened. Anton will take this action item. This is specific to vendors. – No Updates (remove)
 - e. Gavin – Send team the verbiage for “levels/type of actions” to be taken by the team for agreement and adoption – Mike and Gavin are working on this. The draft has been sent but did not include CVSS score. They will send the document out when it is completed. – Mike Scheck wrote up a document that includes the levels/type of actions along with CVSS scoring. Gavin has proofed the document to remove any company specific references and sent it out to the team. Gavin will have it published on FIRST (action item)
 - f. Mike C. – Provide comments and feedback to the team from his meeting with Microsoft – Mike C provided an update regarding his meeting with Microsoft. Microsoft is going to start to participate with the team. Also they are going to collect comments and provide to us. Microsoft has concerns about adding the CVSS scores to their advisories. They need to be added to the mailer. Mike will provide the email addresses.
 - g. Catherine – Confirm that Bryan Banta is available to tabulate the scores. – Bryan has written the front-end to save the scores. There are still some things missing. A meeting will need to be scheduled to gather the requirements. Gavin has someone who can enter the data. – No update
 - h. Gavin – Follow up on date, time and topic for In-person meeting at FIRST TC On November 14-15th in Redwood City, CA – Many are unable to attend in person. Should we have the meeting in person? Gavin will send an email to the mailer to see who can attend – In person meeting cancelled.
 - i. Mike S. – Have a friend working on a CVSS Logo – The logo is okay. The colors seemed to be washed out and maybe something can be done with CVSS by using fonts. Team agreed that it should be worked on more.
- 3) CVSS Structure, Strategy and Process:
- a. Methodology for incorporating feedback into CVSS –
 - Capture the energy of this group with weekly or bi-weekly change proposals. Lead time for the proposed change and implementation to be two weeks. Is this enough time to look at the proposal and agree?
 - Hesitant to change any scoring. Keep the past vulnerabilities scored to the CVSS it is based on. The scoring has been working out.
 - Adopt a new way of tracking changes. Work out a structure to be published. Use a real example
 - Team to look over the email Andrew sent on this subject
 - b. Scoring:
 - None (just send packets; connect to 80/tcp, etc)
 - Registered (register for forum, authentication to service, no identity verification)
 - Authenticated (intended to have credentials - sysadmin created them)
 - i. Pete made a request when doing manual scoring to do a comparison with the scores done by NIST.
 - ii. We are not doing the scoring on a regular basis. Recommend changing it from 5 a week to 1 a week.
 - iii. Pete will send one from the NIST list a week.

- iv. Team to score the one vulnerability. If any issues encountered with the scoring; document and explain the issue to be discussed by team
- c. Scoring Comparison – See 3b
- d. Scoring Examples – Adding additional examples; who do we get to add them in – See 3b
- e. Testing (was scheduled to end on November 4th) – Testing will continue until the team feels enough information has been gathered.
- 4) Administrative:
 - a. Status on groups sharing scoring vulnerabilities – No updates
 - b. CVSS v1.x documentation status update and proposed changes – No Updates
 - c. CVSS Logo – Do we adopt? – See 2i
 - d. National Vulnerability Database CVSS Support – Would like to go public with this after Thanksgiving Holiday. Gavin will help Pete with the press announcement. Gavin will also do checks on the scores and provide feedback.
- 5) Roundtable: Updates/Needs/Questions

Action Items:

- 1) Mike C – Look into search capabilities on the Mailer
- 2) Gavin – Send email to get a volunteer for the “Own Best Practices documentation”
- 3) Gavin – Publish “levels/type of actions” document to FIRST site.
- 4) Mike C. – Provide email addresses for Microsoft to be added to mailer.
- 5) Catherine – Confirm that Bryan Banta is available to tabulate the scores. – Bryan has written the front-end to save the scores. There are still some things missing. A meeting will need to be scheduled to gather the requirements. Gavin has someone who can enter the data.
- 6) Mike S./Team – Continue work on a CVSS Logo
- 7) Gavin/Andrew - Methodology for incorporating feedback into CVSS (adopt new way to track changes)
- 8) Pete – Send one vulnerability a week to team to be scored
- 9) Gavin/Pete – Work on press announcement
- 10) Gavin – Do checks NIST scoring and provide feedback to Pete