Meeting Minutes CVSS
Date: Tuesday 28th of June 2005:

Attendance: 30

Agenda: CVSS BOF session
Go over CVSS with FIRST members

++
Gavin Reid opens the meeting
He explains he would like people to start scoring vulnerabilities and link them to the remediation steps taken. He needs volunteers.

He sees three options
1. Score all vulnerabilities and report these back to group
2. All score the same 3, 4 vulnerabilities and report back the actions taken (Problem might be not all vulnerabilities are appropriate and accurate for different environments (companies, universities, ..)
3. Take 20, 30 vulnerabilities from last year and score those

Cath:
Would like to compare and discuss scoring with different companies to get a baseline. Connect scores to actions, real data. It will help us evaluate the maturity of the model also.

Steve Lippner from Microsoft created the Microsoft vulnerability systems. He found it's essential to take 100% of all vulnerabilities over a couple of years and then compare. However, this would still not lead to a perfect system.
For our test, he suggested picking a few hundred over a year and these should be completely random (!) ones.

Art Manion explained that the environmental scores may be very different and are essentially incomparable

Ben from Siemens wonders how he can view the status of different vulnerabilities. What will happen after one year of scoring?

Gavin explained it's a numerical arbitrary system and is not sure where it will lead us. It needs testing and is not mature yet. He would like to initially freeze it for 6 months, and then see if there are changes required.

Ben from Siemens wonders about the scoring. For example, ISP's don't care about confidentiality but banks would - how can we compare these scores?

Mike from Cisco explains this is currently not possible either but this is an effort to make them comparable. Vendors will rate impact. There is currently no standard between different vulnerability systems either

Mike explained there are company specific bits in CVSS (the environmental score) which will lead to different scores for different types of companies, universities,..

Florian stated there is a fundamental problem: We can't honor availability against confidentiality. Single number cannot service guidelines for all. Different entities will always rate differently.

Gavin agreed this is true, different companies may rate scores differently and act differently. This is untested.

Catherine mentioned that balancing the scores among different companies could average out the scores.

Gavin said that CVSS is great for the average user to figure out and make a value decision on vulnerability.
Catherine also said that CVSS can help smaller teams judge vulnerabilities easier.

The idea is, as Mike stated that in version 1, we have to test the scoring and see if anything's missing. This will lead to a better version 2. There's a balance between over-simplification and making it simple enough to understand

Catherine added there's also a balance between too much and too little info. It would not necessary provide more info on the risk

Question from the audience: Will CVSS be implemented across version vendors?

Catherine: CVSS could be a common ground across the industry

Rakesh asked the audience: What do they do now?
Jerry: we use a matrix. He liked the fact that scores comes from vendor as they know their product best, but that also environmental variables are included
Art:: I know 4,5 companies have something like this. We normalize nothing, we do our own and make our own call.
Steve: that is biased and influenced by infrastructure. Does CVSS take out the bias?
Art: there always be some subjectivity
Mike: CVSS only rates impact on device, not where it is used.

On the subject of published exploit code, Steve said: published exploit is same as a rampant worm

Mike stated that the vendor is most qualified to rate their own vulnerabilities but that the level of detail is inconsistent per vendor. More detail will allow you to rate vulnerability better.

Gavin said that to him, actions matter most – at the same time very different scores (2 vs. 9) would be worth investigating also

Derek, SUN thinks that vendors should not give you a CVSS number but rather the details to make your own. He thinks that his customers will not believe his score.
There should be enough details to help good – but little enough info not to help the bad guys. There should be a balance there.

Rakesh: If CVSS would become trusted, it will help to rate risk. Currently, there is no general, useful system. We need something actionable.

Ben from Siemens thinks we are making the abstraction too early. We are aiming at the number of systems but should rather base CVSS on the type of environment (company, university,..) and use it as a bias system for that

Catherine: If Sun had CVSS score of X and another company had a lower score Y, conservative scores could be used as marketing tool "as it must be safer"

Gavin agreed we need some kind of backup to make sure there is no manipulation

Jerry said that the end user cannot get a final number from vendor. The vendor might provide 1 and 2 but the end user does 3 .. to get at least a subjective view of the environment

Jerry: Is there support from core vendors?
Mike: There are some legal implications ... they could be sue dif scored to low or high. Under investigation.

Other ideas:
- Integrate with vulnerability scanning - leverage CVSS to see what are the risk (Matthew Bing, Michigan)

Gavin closes of the meeting by noting: CVSS is for end users and the reason for this BOF was to check the interest of vendors.
What we have done so far:
- For overall feedback , we created a master list of issues which may be resolved in version 2.0
- There are two mailing lists of which cvss-info@first.org is the public one. Please sign up at first-sec@first.org to subscribe
- http://www.first.org/cvss has more details on CVSS

Volunteers after the meeting:
Hans Ulmer Hans.ulmer@sap.com
Michael Hartmann Michael.Hartmann@sap.com
Jerry Bongard jbongard@csc.com

Hessel Heerebout

Cisco Systems, CSIRT