Network Security

AA 2015/2016

Scoring exercise

Dr. Luca Allodi

Scoring variance – example from last time

- CVE-2009-0927
  - Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1, 8 before 8.1.3 , and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getIcon method of a Collab object, a different vulnerability than CVE-2009-0658.

Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

An alternative score for this vuln exists.
If one assumes that the vuln requires some pdf file to be opened by A.Reader, then we have:

- AV:L/UI:R

In this case we went with the one that gives the higher severity (AV:N,UI:N)

Imperfect scoring

- Vulnerability assessments are carried out by humans
  - Not an automated or fully formalised process
  - Outcome may depend on a number of factors
- CVSS v3 is the result of a huge effort (among others) to devise the definition language to minimise
  - Scoring complexity
  - Variance in the interpretation of the definitions
- Yet, some metrics may induce a higher scoring variance than others
  - Problems with its definition?
  - May vary depending on other external factors

Improving a standard

- UniTn → part of the standard body for CVSS
- Three main questions:
  - Which metrics cause the highest variance in the final scoring?
    - How to improve the metric definitions?
  - Which "external" factors contribute to a "precise" or "consistent" scoring?
    - The vulnerability description?
    - Security vs sw engineering expertise?
    - Formal knowledge about security?
  - Does the perceived severity of a vulnerability match that estimated by the CVSS formula?

Today's class

- Outcome of today's class is twofold
  1. Give you the opportunity to have a full immersion in the standard
     - Critical skill for security professionals in most roles
     - Useful practice for the Network Security final exam
  2. Collect data to identify ways to improve the standard
     - Your analyses will be used to evaluate the influence to scoring variance of factors such as
       - Security expertise
       - Formal security-related education
       - Vulnerability definitions
- Two steps
  1. Questionnaire → useful to estimate "security expertise" and background
  2. Scoring exercise

Questionnaire

- Connect to Google Classroom
- Assignment with questionnaire is online
  - Compile it using your browser
  - Should not take more than 10 minutes
- If you already participated in the “pilot” of this experiment, answer “yes” to question 7
  - You will be considered “experts with previous experience” in this study (which has different vulns from previous one)

→ info used to estimate security expertise and education

Scoring exercise

- Each of you has been assigned to **only one** of four exercises: A,B,C,D
  - Each group differs only for the arrangement of the vuln description
  - All have identical vulnerabilities to score
- **→ the different exercises will tell us if vulnerability definitions help with the scoring correcteness**
- 16 vulnerabilities to score
  - Should take less than 1 hour
  - At the end we will go through the scoring to discuss opinions.
- **Check your exercise assignment on classroom in the file**
  - **"cvss exercise assignment.xlsx"**

Additional fields

- Estimated score: 1-10 with 10 very bad, 1 not so bad
- Impact → remember to score the "first bad thing"
- Confident?
  - Yes=the vuln is clear to me
  - No= I'm not sure
- DK → Domain Knowledge:
  - 0: I have bearly heard of that software, don't know it
  - 1: I have some knowledge on what the software does
- Comments
  - Leave comments on the vulnerability.
    - Was the provided information sufficient?
      - If not, what additional info you deem necessary?
    - Is there something you did not understand?