CVSS – Main Survey – Questionnaire

Readme: Questionnaire for the main survey for the paper “Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities”. *Texts in italics* in brackets are internal question codes and provide additional information.

Welcome Message

Thank you for your interest in this survey, which is designed to evaluate the reliability of CVSSv3.1. This survey is intended for people who are currently assessing vulnerabilities using CVSS. The survey will be running till February 15, 2021.
Please try to answer every question, as only a completed survey is valuable to us. Your answers will be anonymised and handled with care. The survey takes 30 min on average (according to participation times measured so far).
It consists of four parts:

1. Brief questions about your CVSS experience
2. Four security issues we would like you to evaluate using CVSSv3.1
3. Brief questions about your opinion on CVSS
4. Demographic questions

For this survey to work properly, you need to have JavaScript activated in your browser. The survey was created by the IT Security Infrastructures Lab of the Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). If you have any questions, please contact Julia Wunder (julia.wunder@fau.de).

Participation consent

(participationConsent, single choice)
I hereby consent to participating in this survey. The goal of this survey is to evaluate the reliability of CVSSv3.1 and to evaluate the quality of descriptions of vulnerabilities. I also consent that my survey data will be collected, processed and used by the Friedrich-Alexander-Universität Erlangen-Nürnberg for research purposes. I may abort the survey at any time and delete my answers without any disadvantages. For further processing of the collected data, all information will be anonymised.

- I consent.
- I do not consent.

Introductory Question

(filterCurrentlyCVSS, single choice)
Are you currently assessing vulnerabilities using CVSS?

- Yes
- No

(If this question is answered with “No”:)
This survey is intended for people who are currently assessing vulnerabilites using CVSS. As you answered the corresponding question with “No”, this survey is not suitable for you. We apologize for the inconvenience.

If you know people suitable for paticipation in this survey, please forward the link to the survey to them, distribute it on mailing lists and social media. Thank you!

Survey on reliability of CVSS assessments by the University of Erlangen, Germany:
(Survey link)

Your work experience

(currentPosition, free text)
What is your current job title or position?

(yearsCurrentPosition, free text, digits only)
Please estimate how many years you have been working in your current position.

(expertise, single choice for each option)
Please assess your expertise in the following areas:
(Answer options: None, Basic, Intermediate, Advanced, Expert)

- System Software Security

- Desktop Application Software Security
- Mobile Application Software Security
- Web Application Software Security
- Database Security
- Embedded Systems Security
- Network Security
- Product Security

(expertiseOther, free text)
If you have advanced or expert level of expertise in some other security areas, please provide them here:

(yearsITSecurity, free text, digits only)
Please estimate how many years you have been working in the IT security sector.

(yearsCVSS, free text, digits only)
Please estimate how many years you have been working with CVSS.

(selfAssessmentCVSS, single choice for each option)
Please assess your knowledge of CVSS:
(Answer options: None, Basic, Intermediate, Advanced, Expert)
- CVSSv3.1
- CVSSv3.0
- CVSSv2

(trainingFIRST, single choice for each option)
FIRST offers special courses to get familiar with CVSS. Have you participated in the following FIRST e-learning CVSS courses?
(Answer options: Yes, No)
- FIRST Mastering CVSS v3.1
- FIRST Mastering CVSS v3.0

CVSS at your work

(dailyCVSSVersion, multiple choice)
What are your default CVSS versions for daily tasks?
- CVSSv3.1
- CVSSv3.0
- CVSSv2
- I don’t have a default CVSS version.
- I don’t use CVSS for my daily tasks.

(workCVSScustomer, multiple choice)
For whom do you assess vulnerabilities using CVSS?
- For customers (e.g., for other companies)
- Internally (e.g., for your own company, for yourself)
- Other, please indicate: *(free text)*
- I don’t assess vulnerabilites.

(workCVSSUse, multiple choice)
How is CVSS used at your work?
- Prioritising vulnerabilities
- Assessing the severity of vulnerabilities
- Assessing the risk of vulnerabilities
- Other, please indicate: (*free text)*
- I don’t know.
- We don’t use CVSS

(workBaseScoreUse, single choice)
How is the CVSS Base Score used at your work primarily?
- The Base Score is used without adaptation.
- The Base Score is adapted by the Environmental Score.
- The Base Score is adapted by the Temporal Score.
- The Base Score is adapted by the Environmental and Temporal Score.

- Other, please indicate: (*free text)*
- I don’t know.
- We don’t use the Base Score.

(aidsCVSS, multiple choice)
What documents or tools are you using during a CVSS assessment?
- Online-Calculator (e.g., FIRST’s CVSS-Calculator)
- FIRST’s Specification Document for CVSS
- FIRST’s User Guide for CVSS
- FIRST’s Examples Document for CVSS
- Internal company specific documents and software
- Other, please indicate: (*free text)*
- Nothing

(timeEvaluation, free text, digits only)
Please estimate your average time (in minutes) spent per security issue while evaluating using CVSS.

(numberCVSSAssess, free text, digits only)
Please estimate the number of security issues you are evaluating using CVSS on average per week.

(numberPersCVSSAssess, free text, digits only)
How many persons (including yourself) are usually involved in an evaluation using CVSS at your work?

(reactionAmbiguity, multiple choice)
If you are unsure about a CVSS assessment, what or whom do you consult?
- FIRST’s Specification Document for CVSS
- FIRST’s User Guide for CVSS
- FIRST’s Examples Document for CVSS
- Internet research (e.g., Google, Stack Overflow)
- This is an attention test. Please check this item additionally to any other items that you checked here.
- Ratings of the same issue by other parties
- Ratings of similar issues
- Ask coworkers
- Other, please indicate: (*free text)*
- I don’t consult anybody or anything.

(baseScoreReviewCowor, single choice)
Are Base Scores that you calculated reviewed or verified by coworkers or other people?
- Always
- Often
- Occasionally
- Rarely
- Never
- I don’t know

FIRST’s official documents of CVSS

(knowledgeFIRSTsDoc, single choice for each option)
Please assess your knowledge of FIRST’s official documents of CVSS:
(Answer options: None, Basic, Intermediate, Advanced, Expert)
- Specification Document CVSSv3.1
- User Guide CVSSv3.1
- Examples Document CVSSv3.1
- Specification Document CVSSv3.0
- User Guide CVSSv3.0
- Examples Document CVSSv3.0
- User Guide CVSSv2
- Examples Document CVSSv2

(lastConsultFIRSTsDoc, single choice for each option)
Please indicate when you have last consulted FIRST’s official documents:
(Answer options: Never, More than a year ago, A few months ago, A few weeks ago, A few days ago or today)
- Specification Document CVSSv3.1

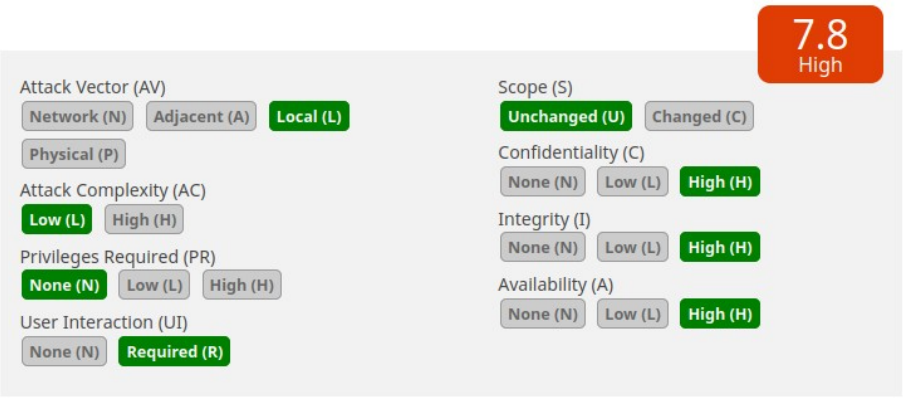
- User Guide CVSSv3.1
- Examples Document CVSSv3.1
- Specification Document CVSSv3.0
- User Guide CVSSv3.0
- Examples Document CVSSv3.0
- User Guide CVSSv2
- Examples Document CVSSv2

CVSS scoring assessment

On the following pages, you will be asked to calculate CVSS 3.1 scores for four security issues using an online calculator. Please leave a comment sharing your assumptions about the calculation of the security issue. Please also share your thoughts on whether there were any ambiguities or other issues with the description or scoring process.
This study evaluates the reliability of CVSSv3.1 and not the skills of the survey participants. Important: Please do not try to get additional information about the security issues. Use only the supplied description as information.

Security Issue
(This part of the survey asked the participants to evaluate four vulnerabilities with randomized order using CVSSv3.1. The same questions were asked for each vulnerability, therefore, only one of the vulnerabilities is described in the following text.)

"Studio in Open edX Ironwood 2.5 allows users to upload SVG files via the „Content>File Uploads" screen. These files can contain JavaScript code and thus lead to Stored XSS."



([vulnerability]vector, e.g. storXSSvector)
Please use this embedded version of FIRST's Online Calculator to compute the Base Score.

The vector string will appear in the text box below once you have chosen all metrics.

([vulnerability]assumptions, free text)
If you relied on any special assumptions in your assessment please state them here.

([vulnerability]confi, single choice for each option)
Please indicate your agreement with the following statements:
(Answer options: Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly agree)
- I'm fully confident in my calculation of the Base Score.
- I know what the software described in the security issue does.
- The description of the security issue is clear and understandable.
- The described security issue is fully suitable for an evaluation using CVSS.
- I often evaluate security issues of this type in my daily work.
- This is an attention test. Please click "Agree" here. *(This option is only displayed for one scoring assessment)*

([vulnerability]comment, free text)
Please leave a comment in case there was an ambiguity or any other issues with the description or the calculation of the security issue. If you think CVSS is unsuitable to evaluate this security issue, please explain why.

CVSS usage questions
(The following questions and answer choices were randomized for each participant. "correct" means here that the CVSS documentation guides (specification, user guide, examples for CVSSv3.1) to act or evaluate in this way.)

(worstRealisticEval, single choice)
In case of a CVSS assessment I usually evaluate the impact metrics considering. . .
- . . . a realistic scenario (e.g., software or company specific characteristics).
- . . . the reasonable worst case scenario. *(correct)*
- Other, please indicate: *(free text)*
- I don't understand this question.

(advKnowEval, single choice)
If an attacker requires advanced knowledge to exploit the vulnerability, I usually evaluate the vulnerability assuming. . .
- . . . the attacker already has advanced knowledge. *(correct)*
- . . . the attacker does not yet have the advanced knowledge.
- Other, please indicate: *(free text)*
- I don't understand this question.

(specConfigEval, single choice)
If a system needs to be in a specific configuration in order to exploit the vulnerability, I usually evaluate assuming. . .
- . . . the system is not in this specific configuration and the attacker accordingly needs to prepare the system.
- . . . the system is already in this specific configuration. *(correct)*
- Other, please indicate: *(free text)*
- I don't understand this question.

(socialEngEval, single choice)
If Social Engineering is required in order to exploit the vulnerability, I usually adapt. . .
- . . . the User Interaction metric. *(correct)*
- . . . the Privileges Required metric.
- . . . none.
- Other, please indicate: *(free text)*
- I don't understand this question.

(privRequEval, single choice)
If an attacker can cause moderate damage with unprivileged user rights or can cause serious damage with admin rights, I usually evalutate the Privileges Required metric as. . .
- Privileges Required: None.
- Privileges Required: Low.
- Privileges Required: High. *(correct)*
- Other, please indicate: *(free text)*
- I don't understand this question.

(scopeChangeEval, single choice)
If a scope change (S:C) occurred, I usually evaluate the impact on. . .
- . . . the vulnerable component.
- . . . the impacted component.
- . . . the component which suffers the most severe outcome. *(correct)*
- Other, please indicate: *(free text)*
- I don't understand this question.

(availabilityEval, single choice)
The metric Availability reflects the availability of. . .
- . . . performance and operation of the impacted component. *(correct)*
- . . . data used by the impacted component.
- . . . data, performance and operation of the impacted component.
- Other, please indicate: *(free text)*
- I don't understand this question.

Your opinion about CVSS

(opinionCVSSUse, multiple choice)
In your opinion, how should CVSS be used?
- Assessing the severity of vulnerabilities
- Assessing the risk of vulnerabilities
- Prioritising vulnerabilities
- Other, please indicate: *(free text)*

(opinionBaseScoreUse, single choice)
In your opinion, how should the Base Score be used primarily?
- The Base Score should be used without adaptation.
- The Base Score should be adapted by the Environmental Score.
- The Base Score should be adapted by the Temporal Score.
- The Base Score should be adapted by the Environmental and Temporal Score.
- Other, please indicate: *(free text)*

(usabilityCVSS, single choice for each option, all question options were randomized for each participant)
Please indicate your agreement with the following statements:
(Answer options: Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly agree)
- CVSS is useful for vulnerability management.
- CVSS is helpful for assessing vulnerabilities.
- CVSS scores are useless.
- CVSS is hard to learn.
- CVSS scores are easy to calculate after understanding the vulnerabilities.
- CVSS evaluations require low effort.
- CVSS evaluations take little time.
- There is too much inconsistency in CVSS.
- I feel confident using CVSS.
- CVSS scores differ depending on who calculates.
- I like using CVSS.
- I feel dissatisfied with CVSS.
- Personally, I would like to use CVSS in the future.
- This is an attention test. Please click “Agree” here.

Demographic questions

The following questions are important for this research to assess the representativeness of the survey.

(gender, single choice)
Please indicate your gender.
- Male
- Female
- Diverse
- Prefer not to say

(yearOfBirth, dropdown menu with years from 1920 to 2005, Prefer not to say)
Please indicate your year of birth.

(residence, dropdown menu with all countries, Prefer not to say)
Please indicate your country of residence.

(occupation, single choice)
Please indicate your current main occupation.
- Employee, civil servant
- Self-employed (with employees)
- Freelancer
- Student
- Other, please indicate: *(free text)*
- Prefer not to say

(educationSchool, single choice)
Please indicate your highest school education level.

- No school certificate
- Primary school/elementary school or equivalent
- Middle school/secondary school or equivalent (not meeting university entrance requirements)
- High school or equivalent (meeting university entrance requirements)
- Other, please indicate: *(free text)*
- Prefer not to say

(educationUniversity, single choice)
Please indicate your highest completed academic/professional education level.
- No completed academic/professional education
- Completed vocational training
- Bachelor's degree or equivalent
- Master's degree or professional degree (M.D., J.D., etc.) or equivalent
- Ph.D. (doctoral degree)
- Other, please indicate: *(free text)*
- Prefer not to say

(numberPeopleCompany, single choice)
Please estimate how many people are employed at your work.
- 1-9
- 10-49
- 50-249
- 250-499
- 500-999
- 1,000-4,999
- 5,000-9,999
- 10,000 or more
- I don't know.
- Prefer not to say

(economicSectorComp, single choice)
Please indicate the economic sector of your company or organization.
- Accommodation and food service activities (e.g., hotel, camping grounds, restaurants, event catering)
- Administration and support service activities (e.g., rental leasing, employment activities, office administrations)
- Agriculture, forestry and fishing
- Arts, entertainment and recreation
- Construction (e.g., construction of buildings, civil engineering, demolition)
- Education
- Electricity, gas, steam and air-conditioning supply
- Financial and insurance activities
- Human health services, residential care and social work activities
- Information and communication (e.g., publishing activities, programming, information service activities)
- Manufacturing (e.g., manufacturing of food, textiles, chemical products, electronics, machinery)
- Mining and quarrying
- Professional, scientific, technical activities (e.g., legal, accounting, research & development, technical testing and analysis)
- Public administration and defence, compulsory social security
- Real estate activities (e.g., buying, selling and renting real estates)
- Transportation and storage (e.g., passenger transport, warehousing, postal and courier activities)
- Water supply, sewerage, waste management and remediation
- Wholesale and retail trade, repair of motor vehicles and motorcycles
- I don't know.
- Other, please indicate: *(free text)*
- Prefer not to say

(nameCompany, free text)
If possible, please provide the name of your company. This information will not be published and will be only used internally to correlate answers of people from the same company.

Feedback

(control, single choice for each option)
Please give us feedback on the completion of this survey:
(Answer options: Strongly disagree, Disagree, Agree, Strongly agree)

- I was distracted during the questioning (e.g., phone calls, other people, ...).
- I have answered the questions carefully.
- I consulted FIRST's official CVSS documents during this survey.
- I tried to get additional information about the security issues (e.g., used Google, asked other people, ...).

(feedback, free text)
If you would like to give us additional feedback on the survey, please share it here.

(CVSSthoughts, free text)
If you have any thoughts on CVSS which were not covered by this survey, please share them in the text box below.

(informedSurvey, single choice)
Would you like to be informed about the results of this survey?

- Yes
- No

(followUpSurvey, single choice)
May we contact you for a short follow-up CVSS survey?

- Yes
- No

(eMailParticipant, free text)
If you answered "Yes" to at least one of the questions above, please provide a contact email address here. The provided email address will be used solely for the purposes you indicated above and for nothing else. It will be deleted after the completion of this research project.

End Message

Thank you for participating in this survey.
Please help us to distribute this survey. If you know people suitable for participation in this survey, please forward the link to the survey to them, distribute it on mailing lists and social media. Thank you!

Survey on reliability of CVSS assessments by the University of Erlangen, Germany:
(Survey link)

The survey was created by the IT Security Infrastructures Lab of the Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). If you have any questions please contact Julia Wunder (julia.wunder@fau.de).