CVSS – Follow-up Survey – Questionnaire

Readme: Questionnaire for the follow-up 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

This follow-up survey is based on the previous CVSS survey you participated in. It investigates further aspects about the reliability of CVSSv3.1. The survey takes 15 minutes on average.
Like in the previous survey we would like you to evaluate four security issues using CVSSv3.1 and answer some questions. Your answers will be anonymized and handled with care.

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.

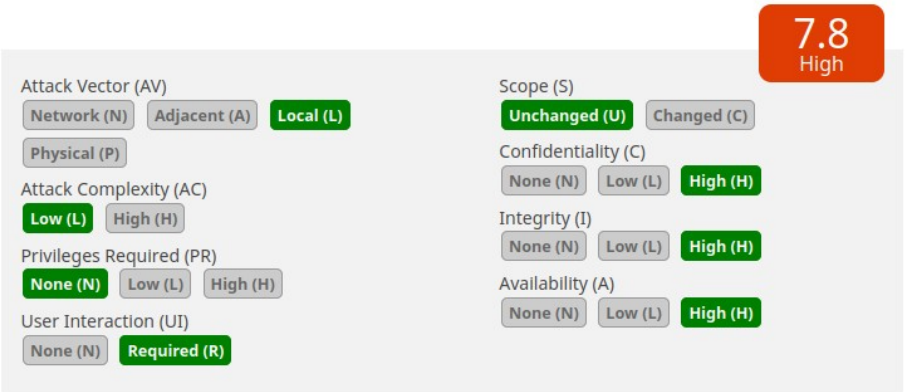
CVSS scoring assessment

On the following pages, you will be asked to calculate CVSS 3.1 scores for four security issues using an online calculator. If some of them seem familiar to you from the previous survey, please evaluate them according to your current opinion.
This study evaluates the reliability of CVSSv3.1 and not your skills. Therefore, there are no wrong or right answers.

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.

([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.

([vulnerability]LastSeen, single choice)
(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes
- No
- I'm not sure

CVSS questions

(CVSSversions, single choice for each option)
Over the years different versions of CVSS have been developed: CVSSv2, CVSSv3.0 and CVSSv3.1. Please indicate your agreement with the following statement:
(Answer options: Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly agree)

- Differences in versions of CVSS often cause problems and discussions.

(metricProblem, single choice for each option)
Please indicate your agreement with the following statement for each metric: The evaluation of this metric often leads to problems and discussions:
(Answer options: Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly agree)

- Attack Vector (N, A, L, P)
- Attack Complexity (L, H)
- Privileges Required (N, L, H)
- User Interaction (N, R)
- Scope (U, C)
- Confidentiality (N, L, H)
- Integrity (N, L, H)
- Availability (N, L, H)

(CVSSthoughts, free text)
If you have any additional comments, please share them in the text box below.

End Message

Thank you for participating in this follow up survey and helping us to evaluate the reliability of CVSSv3.1.

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).