CVSS – Main Survey – Results

Readme: Contains the descriptive results for the main survey for the paper “Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities”. Comments and free text answers are not included. *Texts in italics* in brackets are internal question codes and provide additional information.
In total 207 people completed the main survey. Ten were excluded because they did not pass the attention tests, and one was under 18, which leaves 196 valid answers.

Your work experience

(yearsCurrentPosition)
Please estimate how many years you have been working in your current position.

- Min.: 1
- Max.: 22
- Median: 5
- Average: 5.94

(expertise)
Please assess your expertise in the following areas:

	None	Basic	Intermediate	Advanced	Expert
System Software Security	5	25	46	82	38
Desktop Application Software Security	9	38	61	71	17
Mobile Application Software Security	22	76	56	33	9
Web Application Software Security	3	29	37	71	56
Database Security	11	61	67	48	9
Embedded Systems Security	38	65	43	36	14
Network Security	2	10	53	87	44
Product Security	10	30	55	72	29

(yearsITSecurity)
Please estimate how many years you have been working in the IT security sector.

- Median: 10
- Average: 11.29

(yearsCVSS)
Please estimate how many years you have been working with CVSS.

- Median: 5
- Average: 6.18

(selfAssessmentCVSS)
Please assess your knowledge of CVSS:

	None	Basic	Intermediate	Advanced	Expert
CVSSv3.1	10	29	60	74	23
CVSSv3.0	12	23	67	68	26
CVSSv2	26	49	56	44	21

(trainingFIRST)
FIRST offers special courses to get familiar with CVSS. Have you participated in the following FIRST e-learning CVSS courses?

	Yes	No
FIRST Mastering CVSS v3.1	12	184

CVSS at your work

(dailyCVSSVersion, multiple choice)
What are your default CVSS versions for daily tasks?
- CVSSv3.1: 119
- CVSSv3.0: 75
- CVSSv2: 26
- I don’t have a default CVSS version.: 14
- I don’t use CVSS for my daily tasks.: 11

(workCVSScustomer, multiple choice)
For whom do you assess vulnerabilities using CVSS?
- For customers (e.g., for other companies): 113
- Internally (e.g., for your own company, for yourself): 144
- Other, please indicate: *(free text): 8*
- I don’t assess vulnerabilites.: 0

(workCVSSUse, multiple choice)
How is CVSS used at your work?
- Prioritising vulnerabilities: 117
- Assessing the severity of vulnerabilities: 165
- Assessing the risk of vulnerabilities: 110
- Other, please indicate: (*free text)*: 19
- I don’t know.: 0
- We don’t use CVSS: 0

(workBaseScoreUse, single choice)
How is the CVSS Base Score used at your work primarily?
- The Base Score is used without adaptation.: 108
- The Base Score is adapted by the Environmental Score.: 26
- The Base Score is adapted by the Temporal Score.: 14
- The Base Score is adapted by the Environmental and Temporal Score.: 25
- Other, please indicate: (*free text)*: 14
- I don’t know.: 3
- We don’t use the Base Score.: 6

(aidsCVSS, multiple choice)
What documents or tools are you using during a CVSS assessment?
- Online-Calculator (e.g., FIRST’s CVSS-Calculator): 150
- FIRST’s Specification Document for CVSS: 51
- FIRST’s User Guide for CVSS: 47
- FIRST’s Examples Document for CVSS: 39
- Internal company specific documents and software: 87
- Other, please indicate: (*free text)*: 11
- Nothing: 4

(timeEvaluation)
Please estimate your average time (in minutes) spent per security issue while evaluating using CVSS.
- Median: 5
- Average: 25.20

(numberCVSSAssess)
Please estimate the number of security issues you are evaluating using CVSS on average per week.
- Median: 10
- Average: 58.83

(numberPersCVSSAssess)
How many persons (including yourself) are usually involved in an evaluation using CVSS at your work?
- Median: 3

- Average: 11.41

(reactionAmbiguity, multiple choice)
If you are unsure about a CVSS assessment, what or whom do you consult?
- FIRST's Specification Document for CVSS: 83
- FIRST's User Guide for CVSS: 59
- FIRST's Examples Document for CVSS: 48
- Internet research (e.g., Google, Stack Overflow): 106
- Ratings of the same issue by other parties: 87
- Ratings of similar issues: 109
- Ask coworkers: 127
- Other, please indicate: (*free text)*: 16
- I don't consult anybody or anything.: 2

(baseScoreReviewCowor, single choice)
Are Base Scores that you calculated reviewed or verified by coworkers or other people?
- Always: 67
- Often: 40
- Occasionally: 44
- Rarely: 28
- Never: 12
- I don't know: 5

FIRST's official documents of CVSS

(knowledgeFIRSTsDoc)
Please assess your knowledge of FIRST's official documents of CVSS:

	None	Basic	Intermediate	Advanced	Expert
Specification Document CVSSv3.1	51	51	53	33	8
User Guide CVSSv3.1	52	56	46	33	9
Examples Document CVSSv3.1	65	52	47	23	9
Specification Document CVSSv3.0	63	45	44	35	9
User Guide CVSSv3.0	60	50	43	31	12
Examples Document CVSSv3.0	70	51	39	23	13
User Guide CVSSv2	84	57	31	16	8
Examples Document CVSSv2	91	57	26	13	9

(lastConsultFIRSTsDoc)
Please indicate when you have last consulted FIRST's official documents:

	Never	More than a year ago	A few months ago	A few weeks ago	A few days ago or today
Specification Document CVSSv3.1	57	30	60	34	15
User Guide CVSSv3.1	55	29	72	34	6
Examples Document CVSSv3.1	72	28	57	34	5
Specification Document CVSSv3.0	65	69	50	6	6
User Guide CVSSv3.0	63	71	53	7	2
Examples Document CVSSv3.0	76	69	41	6	4
User Guide CVSSv2	90	81	22	2	1
Examples Document CVSSv2	99	74	19	3	1

CVSS scoring assessment - Security Issues
(In total there were 8 scoring assessments. The participants were divided into 2 groups so that each group had to score 4 assessments.)

Reflected XSS – CVE-2019-20512 – Group 1 (97 participants)
Vulnerability: “Open edX in version Ironwood.1 is vulnerable to a reflected XSS attack. An unauthenticated attacker is able to manipulate the HTTP URI parameter /support/certificates?course_id=.”

Metrics:
- Attack Vector: N: 93 A: 0 L: 3 P: 1
- Attack Complexity: L: 85 H: 12
- Privileges Required: N: 92 L: 5 H: 0
- User Interaction: N: 24 R: 73
- Scope: U: 59 C: 38
- Confidentiality: H: 35 L: 48 N: 14
- Integrity: H: 34 L: 52 N: 11
- Availability: H: 11 L: 25 N: 61

Severity:
- None: 3
- Low: 3
- Medium: 49
- High: 31
- Critical: 11

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I’m fully confident in my calculation of the Base Score.	12	20	23	36	6
I know what the software described in the security issue does.	33	22	15	18	9
The description of the security issue is clear and understandable.	8	18	19	39	13
The described security issue is fully suitable for an evaluation using CVSS.	13	20	17	36	11
I often evaluate security issues of this type in my daily work.	7	16	17	38	19

Stored XSS – CVE-2020-13145 – Group 1 (97 participants)
Vulnerability: “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.”

Metrics:
- Attack Vector: N: 88 A: 1 L: 7 P: 1
- Attack Complexity: L: 88 H: 9
- Privileges Required: N: 24 L: 71 H: 2
- User Interaction: N: 40 R: 57
- Scope: U: 59 C: 38
- Confidentiality: H: 46 L: 42 N: 9
- Integrity: H: 48 L: 44 N: 5
- Availability: H: 23 L: 29 N: 45

Severity:
- None: 1
- Low: 3
- Medium: 44

- High: 37
- Critical: 12

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I'm fully confident in my calculation of the Base Score.	12	21	22	37	5
I know what the software described in the security issue does.	33	25	12	21	6
The description of the security issue is clear and understandable.	10	18	1	40	10
The described security issue is fully suitable for an evaluation using CVSS.	14	13	14	42	14
I often evaluate security issues of this type in my daily work.	5	20	15	38	19

SQL Injection – CVE-2020-3184 – Group 1 (97 participants)
Vulnerability: "A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning Software allows an authenticated attacker to conduct SQL injection attacks. The vulnerability exists because the web-based management interface improperly validates user input for specific SQL queries. An attacker can exploit this vulnerability by authenticating to the application with valid administrative credentials and sending malicious requests to an affected system. A successful exploit allows the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, or delete information from the database that they are not authorized to delete."

Metrics:
- Attack Vector: N: 90 A: 5 L: 2 P: 0
- Attack Complexity: L: 80 H: 17
- Privileges Required: N: 3 L: 17 H: 77
- User Interaction: N: 81 R: 16
- Scope: U: 63 C: 34
- Confidentiality: H: 91 L: 6 N: 0
- Integrity: H: 92 L: 5 N: 0
- Availability: H: 70 L: 11 N: 16

Severity:
- None: 0
- Low: 0
- Medium: 25
- High: 52
- Critical: 20

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I'm fully confident in my calculation of the Base Score.	2	11	11	58	15
I know what the software described in the security issue does.	16	21	22	24	14
The description of the security issue is clear and understandable.	2	7	7	61	20

The described security issue is fully suitable for an evaluation using CVSS.	3	7	19	46	22
I often evaluate security issues of this type in my daily work.	2	14	17	39	25

Banner Disclosure – CVE-2020-3193 – Group 1 (97 participants)
Vulnerability: “A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning allows an unauthenticated attacker to obtain sensitive information about an affected device. The vulnerability exists because replies from the web-based management interface include unnecessary server information. An attacker could exploit this vulnerability by inspecting replies received from the web-based management interface. A successful exploit allows the attacker to obtain details about the operating system, including the web server version that is running on the device, which could be used to perform further attacks.”

Metrics:

- Attack Vector: N: 92 A: 4 L: 0 P: 1
- Attack Complexity: L: 87 H: 10
- Privileges Required: N: 95 L: 2 H: 0
- User Interaction: N: 86 R: 11
- Scope: U: 83 C: 14
- Confidentiality: H: 17 L: 69 N: 11
- Integrity: H: 4 L: 8 N: 85
- Availability: H: 3 L: 9 N: 85

Severity:

- None: 9
- Low: 6
- Medium: 68
- High: 11
- Critical: 3

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I’m fully confident in my calculation of the Base Score.	4	12	20	46	15
I know what the software described in the security issue does.	16	23	16	33	9
The description of the security issue is clear and understandable.	5	8	14	48	22
The described security issue is fully suitable for an evaluation using CVSS.	10	17	16	35	19
I often evaluate security issues of this type in my daily work.	5	12	20	40	20

Adobe Acrobat – CVE-2009-0658 – Group 2 (99 participants)
Vulnerability: “Adobe Acrobat and Reader version 9.0 and earlier are vulnerable to a buffer overflow, caused by improper bounds checking when parsing a malformed JBIG2 image stream embedded within a crafted PDF document. The attacker can overflow a buffer and execute arbitrary code on the system with the privileges of the user or cause the application to crash.”

Metrics:

- Attack Vector: N: 39 A: 0 L: 59 P: 1
- Attack Complexity: L: 51 H: 48
- Privileges Required: N: 81 L: 18 H: 0

- User Interaction: N: 14 R: 85
- Scope: U: 60 C: 39
- Confidentiality: H: 71 L: 19 N: 9
- Integrity: H: 75 L: 19 N: 5
- Availability: H: 70 L: 22 N: 7

Severity:
- None: 0
- Low: 2
- Medium: 25
- High: 65
- Critical: 7

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I'm fully confident in my calculation of the Base Score.	2	14	29	48	6
I know what the software described in the security issue does.	0	3	8	44	44
The description of the security issue is clear and understandable.	1	2	13	54	29
The described security issue is fully suitable for an evaluation using CVSS.	3	10	13	58	15
I often evaluate security issues of this type in my daily work.	7	16	19	43	14

Google Chrome – CVE-2016-1645 – Group 2 (99 participants)
Vulnerability: "This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Google Chrome. The specific flaw exists within the handling of JPEG 2000 images. A specially crafted JPEG 2000 image embedded inside a PDF cain preliminary surveyn force Google Chrome to write memory past the end of an allocated object. An attacker can leverage this vulnerability to execute arbitrary code under the context of the current process."

Metrics:
- Attack Vector: N: 70 A: 0 L: 29 P: 0
- Attack Complexity: L: 43 H: 56
- Privileges Required: N: 85 L: 13 H: 1
- User Interaction: N: 17 R: 82
- Scope: U: 62 C: 37
- Confidentiality: H: 71 L: 19 N: 9
- Integrity: H: 74 L: 20 N: 5
- Availability: H: 54 L: 27 N: 18

Severity:
- None: 3
- Low: 2
- Medium: 21
- High: 64
- Critical: 9

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I'm fully confident in my calculation of the Base Score.	2	17	28	47	5

I know what the software described in the security issue does.	0	1	5	55	38
The description of the security issue is clear and understandable.	1	5	16	56	21
The described security issue is fully suitable for an evaluation using CVSS.	0	13	16	58	12
I often evaluate security issues of this type in my daily work.	4	19	22	41	13

MITM MyPalette – CVE-2020-5523 – Group 2 (99 participants)
Vulnerability: “Android App MyPallete and some of the Android banking applications based on MyPallete do not verify X.509 certificates from servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.”

Metrics:
- Attack Vector: N: 66 A: 29 L: 4 P: 0
- Attack Complexity: L: 33 H: 66
- Privileges Required: N: 83 L: 12 H: 4
- User Interaction: N: 53 R: 46
- Scope: U: 75 C: 24
- Confidentiality: H: 83 L: 15 N: 1
- Integrity: H: 58 L: 21 N: 20
- Availability: H: 8 L: 11 N: 80

Severity:
- None: 0
- Low: 4
- Medium: 44
- High: 41
- Critical: 10

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I’m fully confident in my calculation of the Base Score.	1	14	26	52	6
I know what the software described in the security issue does.	7	16	21	36	19
The description of the security issue is clear and understandable.	0	11	14	57	17
The described security issue is fully suitable for an evaluation using CVSS.	2	19	20	51	7
I often evaluate security issues of this type in my daily work.	6	16	17	48	12

HTTPOnly – CVE-2020-27658 – Group 2 (99 participants)
Vulnerability: “Synology Router Manager (SRM) before 1.2.4-8081 does not include the HTTPOnly flag in a Set-Cookie header for the session cookie, which makes it easier for attackers to obtain potentially sensitive information via script access to this cookie.”

Metrics:
- Attack Vector: N: 81 A: 12 L: 6 P: 0
- Attack Complexity: L: 60 H: 39
- Privileges Required: N: 78 L: 16 H: 5
- User Interaction: N: 51 R: 48

- Scope: U: 77 C: 22
- Confidentiality: H: 40 L: 52 N: 7
- Integrity: H: 13 L: 24 N: 62
- Availability: H: 10 L: 9 N: 80

Severity:
- None: 7
- Low: 18
- Medium: 46
- High: 26
- Critical: 2

Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I'm fully confident in my calculation of the Base Score.	7	23	24	39	6
I know what the software described in the security issue does.	6	20	14	39	20
The description of the security issue is clear and understandable.	2	10	16	54	17
The described security issue is fully suitable for an evaluation using CVSS.	11	24	23	39	2
I often evaluate security issues of this type in my daily work.	7	10	15	49	18

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).: 121
- . . . the reasonable worst case scenario. *(correct)*: 65
- Other, please indicate: *(free text)*: 10
- I don't understand this question.: 0

(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)*: 137
- . . . the attacker does not yet have the advanced knowledge.: 31
- Other, please indicate: *(free text)*: 25
- I don't understand this question.: 3

(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.: 65
- . . . the system is already in this specific configuration. *(correct)*: 92
- Other, please indicate: *(free text)*: 38
- I don't understand this question.: 1

(socialEngEval, single choice)
If Social Engineering is required in order to exploit the vulnerability, I usually adapt. . .
- . . . the User Interaction metric. *(correct)*: 159

- . . . the Privileges Required metric.: 12
- . . . none.: 12
- Other, please indicate: *(free text)*: 3
- I don’t understand this question.: 0

(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.: 36
- Privileges Required: Low.: 74
- Privileges Required: High. *(correct)*: 29
- Other, please indicate: *(free text)*: 51
- I don’t understand this question.: 6

(scopeChangeEval, single choice)
If a scope change (S:C) occurred, I usually evaluate the impact on. . .
- . . . the vulnerable component.: 34
- . . . the impacted component.: 64
- . . . the component which suffers the most severe outcome. *(correct)*: 78
- Other, please indicate: *(free text)*: 12
- I don’t understand this question.: 8

(availabilityEval, single choice)
The metric Availability reflects the availability of. . .
- . . . performance and operation of the impacted component. *(correct)*: 74
- . . . data used by the impacted component.: 0
- . . . data, performance and operation of the impacted component.: 112
- Other, please indicate: *(free text)*: 6
- I don’t understand this question.: 4

Your opinion about CVSS

(opinionCVSSUse, multiple choice)
In your opinion, how should CVSS be used?
- Assessing the severity of vulnerabilities: 138
- Assessing the risk of vulnerabilities: 81
- Prioritising vulnerabilities: 118
- Other, please indicate: *(free text)*: 29

(opinionBaseScoreUse, single choice)
In your opinion, how should the Base Score be used primarily?
- The Base Score should be used without adaptation.: 52
- The Base Score should be adapted by the Environmental Score.: 34
- The Base Score should be adapted by the Temporal Score.: 16
- The Base Score should be adapted by the Environmental and Temporal Score.: 63
- Other, please indicate: *(free text)*: 31

(usabilityCVSS, all question options were randomized for each participant)
Please indicate your agreement with the following statements:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
CVSS is useful for vulnerability management.	6	16	28	103	43
CVSS is helpful for assessing vulnerabilities.	5	7	27	115	42
CVSS scores are useless.	76	68	36	8	8
CVSS is hard to learn.	13	76	62	39	6
CVSS scores are easy to calculate after	6	30	55	83	22

understanding the vulnerabilities.					
CVSS evaluations require low effort.	8	60	59	66	3
CVSS evaluations take little time.	3	34	63	83	13
There is too much inconsistency in CVSS.	2	38	59	66	31
I feel confident using CVSS.	3	14	57	109	13
CVSS scores differ depending on who calculates.	0	6	21	96	73
I like using CVSS.	15	21	54	86	20
I feel dissatisfied with CVSS.	19	59	56	44	18
Personally, I would like to use CVSS in the future.	12	12	30	106	36

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: 170
- Female: 7
- Diverse: 1
- Prefer not to say: 18

(yearOfBirth)
Please indicate your year of birth. *(Age as of 2021)*
- Min.: 19 years
- Max.: 63 years
- Median: 36 years
- Average: 38.36 years
- Prefer not to say: 33

(residence)
Please indicate your country of residence.
- Australia: 3
- Austria: 5
- Belgium: 5
- Brazil: 1
- Canada: 1
- Czech Republic: 2
- Denmark: 1
- France: 7
- Germany: 48
- Greece: 1
- India: 2
- Ireland: 1
- Israel: 1
- Italy: 6
- Japan: 1
- Netherlands: 5
- Norway: 1
- Poland: 6
- Portugal: 2
- Romania: 1
- Singapore: 2
- Spain: 2
- South Africa: 1
- Switzerland: 1
- United Kingdom: 25

- United States of America: 38
- Prefer not to say: 27

(occupation, single choice)
Please indicate your current main occupation.
- Employee, civil servant: 165
- Self-employed (with employees): 9
- Freelancer: 3
- Student: 1
- Other, please indicate: *(free text)*: 9
- Prefer not to say: 9

(educationSchool, single choice)
Please indicate your highest school education level.
- No school certificate: 0
- Primary school/elementary school or equivalent: 0
- Middle school/secondary school or equivalent (not meeting university entrance requirements): 5
- High school or equivalent (meeting university entrance requirements): 174
- Other, please indicate: *(free text)*: 9
- Prefer not to say: 8

(educationUniversity, single choice)
Please indicate your highest completed academic/professional education level.
- No completed academic/professional education: 9
- Completed vocational training: 8
- Bachelor's degree or equivalent: 73
- Master's degree or professional degree (M.D., J.D., etc.) or equivalent: 85
- Ph.D. (doctoral degree): 6
- Other, please indicate: *(free text)*: 7
- Prefer not to say: 8

(numberPeopleCompany, single choice)
Please estimate how many people are employed at your work.
- 1-9: 10
- 10-49: 17
- 50-249: 18
- 250-499: 15
- 500-999: 11
- 1,000-4,999: 25
- 5,000-9,999: 12
- 10,000 or more: 70
- I don't know.: 4
- Prefer not to say: 14

(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): 0
- Administration and support service activities (e.g., rental leasing, employment activities, office administrations): 0
- Agriculture, forestry and fishing: 0
- Arts, entertainment and recreation: 1
- Construction (e.g., construction of buildings, civil engineering, demolition): 0
- Education: 2
- Electricity, gas, steam and air-conditioning supply: 2
- Financial and insurance activities: 12
- Human health services, residential care and social work activities: 3
- Information and communication (e.g., publishing activities, programming, information service activities): 87
- Manufacturing (e.g., manufacturing of food, textiles, chemical products, electronics, machinery): 18
- Mining and quarrying: 0
- Professional, scientific, technical activities (e.g., legal, accounting, research & development, technical testing and analysis): 24
- Public administration and defence, compulsory social security: 9
- Real estate activities (e.g., buying, selling and renting real estates): 0

- Transportation and storage (e.g., passenger transport, warehousing, postal and courier activities): 3
- Water supply, sewerage, waste management and remediation: 0
- Wholesale and retail trade, repair of motor vehicles and motorcycles: 0
- I don’t know.: 0
- Other, please indicate: *(free text)*: 17
- Prefer not to say: 18

Feedback

(control)
Please give us feedback on the completion of this survey:

	Strongly disagree	Disagree	Agree	Strongly agree
I was distracted during the questioning (e.g., phone calls, other people, ...).	101	65	27	3
I have answered the questions carefully.	0	1	132	63
I consulted FIRST’s official CVSS documents during this survey.	117	57	19	3
I tried to get additional information about the security issues (e.g., used Google, asked other people, ...).	124	55	17	0

(informedSurvey, single choice)
Would you like to be informed about the results of this survey?
- Yes: 140
- No: 56

(followUpSurvey, single choice)
May we contact you for a short follow-up CVSS survey?
- Yes: 117
- No: 79