CVSS – Follow-up Survey – Questionnaire

Readme: Contains the descriptive results for the follow-up 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 59 people completed the follow-up survey.

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. Each participant evaluated 4 vulnerabilities: two that they already evaluated in the main survey, and two that were evaluated in the main survey by other participants but were new to them.)

Stored XSS – CVE-2020-13145 – Group 1 (32 participants) – Also evaluated in main survey
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: 29 A: 0 L: 3 P: 0
- Attack Complexity: L: 30 H: 2
- Privileges Required: N: 3 L: 29 H: 0
- User Interaction: N: 10 R: 22
- Scope: U: 11 C: 21
- Confidentiality: H: 18 L: 13 N: 1
- Integrity: H: 15 L: 15 N: 2
- Availability: H: 6 L: 8 N: 18

Severity:
- None: 0
- Low: 1
- Medium: 14
- High: 11
- Critical: 6

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	7	6	11	4
I know what the software described in the security issue does.	8	14	2	6	2
The description of the security issue is clear and understandable.	3	10	4	11	4
The described security issue is fully suitable for an evaluation using CVSS.	6	8	2	11	5
I often evaluate security issues of this type in my daily work.	2	4	7	8	11

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?
- Yes: 3
- No: 2
- I'm not sure: 3

MITM MyPalette – CVE-2020-5523 – Group 1 (32 participants) – not evaluated in main survey
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: 23 A: 9 L: 0 P: 0
- Attack Complexity: L: 11 H: 21
- Privileges Required: N: 27 L: 3 H: 2
- User Interaction: N: 18 R: 14
- Scope: U: 25 C: 7
- Confidentiality: H: 26 L: 6 N: 0
- Integrity: H: 21 L: 6 N: 5
- Availability: H: 7 L: 3 N: 22

Severity:

- None: 0
- Low: 1
- Medium: 11
- High: 17
- 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.	2	3	8	15	4
I know what the software described in the security issue does.	8	5	6	10	3
The description of the security issue is clear and understandable.	2	0	2	16	12
The described security issue is fully suitable for an evaluation using CVSS.	2	4	9	11	6
I often evaluate security issues of this type in my daily work.	1	7	9	9	6

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 0
- No: 0
- I'm not sure: 25

Banner Disclosure – CVE-2020-3193 – Group 1 (32 participants) – also evaluated in main survey
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: 29 A: 3 L: 0 P: 0
- Attack Complexity: L: 28 H: 4
- Privileges Required: N: 29 L: 1 H: 2
- User Interaction: N: 30 R: 2
- Scope: U: 28 C: 4
- Confidentiality: H: 4 L: 24 N: 4
- Integrity: H: 2 L: 1 N: 29
- Availability: H: 1 L: 0 N: 31

Severity:

- None: 4
- Low: 0
- Medium: 24
- High: 4
- Critical: 0

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	3	5	10	10
I know what the software described in the security issue does.	4	9	4	13	2
The description of the security issue is clear and understandable.	1	0	2	19	10
The described security issue is fully suitable for an evaluation using CVSS.	3	6	4	11	8
I often evaluate security issues of this type in my daily work.	2	4	8	9	9

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 2
- No: 1
- I'm not sure: 10

HTTPOnly – CVE-2020-27658 – Group 1 (32 participants) – not evaluated in main survey
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: 26 A: 4 L: 2 P: 0
- Attack Complexity: L: 16 H: 16
- Privileges Required: N: 21 L: 7 H: 4
- User Interaction: N: 13 R: 19
- Scope: U: 26 C: 6
- Confidentiality: H: 10 L: 17 N: 5
- Integrity: H: 6 L: 5 N: 21
- Availability: H: 3 L: 3 N: 26

Severity:

- None: 5
- Low: 11
- Medium: 10
- High: 6
- Critical: 0

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.	5	6	6	12	3
I know what the software described in the	4	8	7	10	3

security issue does.					
The description of the security issue is clear and understandable.	1	4	3	16	8
The described security issue is fully suitable for an evaluation using CVSS.	6	8	6	8	4
I often evaluate security issues of this type in my daily work.	2	7	7	7	9

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 1
- No: 0
- I'm not sure: 5

Adobe Acrobat – CVE-2009-0658 – Group 2 (27 participants) – also evaluated in main survey
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: 9 A: 0 L: 18 P: 0
- Attack Complexity: L: 17 H: 10
- Privileges Required: N: 27 L: 0 H: 0
- User Interaction: N: 1 R: 26
- Scope: U: 18 C: 9
- Confidentiality: H: 17 L: 9 N: 1
- Integrity: H: 19 L: 7 N: 1
- Availability: H: 19 L: 8 N: 0

Severity:

- None: 0
- Low: 0
- Medium: 8
- High: 16
- 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.	0	3	5	19	0
I know what the software described in the security issue does.	0	0	0	12	15
The description of the security issue is clear and understandable.	0	1	0	16	10
The described security issue is fully suitable for an evaluation using CVSS.	0	1	1	20	5
I often evaluate security issues of this type in my daily work.	1	2	7	13	4

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 1
- No: 0
- I'm not sure: 5

SQL Injection – CVE-2020-3184 – Group 2 (27 participants) – not evaluated in main survey
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: 25 A: 1 L: 1 P: 6
- Attack Complexity: L: 26 H: 1
- Privileges Required: N: 1 L: 3 H: 23
- User Interaction: N: 26 R: 1
- Scope: U: 18 C: 9
- Confidentiality: H: 23 L: 4 N: 0
- Integrity: H: 24 L: 3 N: 0
- Availability: H: 18 L: 3 N: 6

Severity:

- None: 0
- Low: 1
- Medium: 7
- High: 12
- 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.	0	2	4	15	6
I know what the software described in the security issue does.	2	3	5	13	4
The description of the security issue is clear and understandable.	0	1	2	16	8
The described security issue is fully suitable for an evaluation using CVSS.	0	1	1	16	9
I often evaluate security issues of this type in my daily work.	1	2	5	10	9

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 0
- No: 0
- I'm not sure: 7

Banner Disclosure – CVE-2020-3193 – Group 2 (27 participants) – not evaluated in main survey
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: 25 A: 2 L: 0 P: 0
- Attack Complexity: L: 26 H: 1
- Privileges Required: N: 26 L: 0 H: 1

- User Interaction: N: 25 R: 2
- Scope: U: 19 C: 8
- Confidentiality: H: 4 L: 22 N: 1
- Integrity: H: 0 L: 0 N: 27
- Availability: H: 0 L: 0 N: 27

Severity:
- None: 1
- Low: 0
- Medium: 24
- High: 2
- Critical: 0

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	0	6	13	7
I know what the software described in the security issue does.	1	4	7	11	4
The description of the security issue is clear and understandable.	0	3	2	15	7
The described security issue is fully suitable for an evaluation using CVSS.	1	4	5	12	5
I often evaluate security issues of this type in my daily work.	0	3	4	13	7

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?
- Yes: 0
- No: 0
- I'm not sure: 10

HTTPOnly – CVE-2020-27658 – Group 2 (27 participants) – also evaluated in main survey
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: 22 A: 1 L: 4 P: 0
- Attack Complexity: L: 15 H: 12
- Privileges Required: N: 21 L: 4 H: 2
- User Interaction: N: 14 R: 13
- Scope: U: 19 C: 8
- Confidentiality: H: 12 L: 12 N: 3
- Integrity: H: 7 L: 3 N: 17
- Availability: H: 5 L: 3 N: 19

Severity:
- None: 3
- Low: 5
- Medium: 10
- High: 8
- Critical: 1

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.	0	5	10	11	1
I know what the software described in the security issue does.	1	3	7	9	7
The description of the security issue is clear and understandable.	0	1	6	11	9
The described security issue is fully suitable for an evaluation using CVSS.	5	6	4	9	3
I often evaluate security issues of this type in my daily work.	2	1	4	13	7

(This question only appeared for the last vulnerability for the participant)
Did you evaluate this security issue in our previous CVSS survey?

- Yes: 1
- No: 0
- I'm not sure: 3

CVSS questions

(CVSSversions)
Over the years different versions of CVSS have been developed: CVSSv2, CVSSv3.0 and CVSSv3.1. Please indicate your agreement with the following statement:
Differences in versions of CVSS often cause problems and discussions.

- Strongly disagree: 5
- Disagree: 19
- Neither agree nor disagree: 14
- Agree: 15
- Strongly agree: 6

(metricProblem)
Please indicate your agreement with the following statement for each metric: The evaluation of this metric often leads to problems and discussions:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Attack Vector (N, A, L, P)	8	25	8	14	4
Attack Complexity (L, H)	4	16	10	19	10
Privileges Required (N, L, H)	13	21	11	9	5
User Interaction (N, R)	13	22	8	12	4
Scope (U, C)	0	11	9	15	24
Confidentiality (N, L, H)	5	14	10	22	8
Integrity (N, L, H)	4	16	10	23	6
Availability (N, L, H)	4	12	11	25	7