Rubric for Applying CVSS to Medical Devices

Version: 0.12.04 – September 3, 2019 (revised October 27, 2020)

Steve Christey Coley
coley@mitre.org
Penny Chase
pc@mitre.org

NOTICE

This (software/technical data) was produced for the U. S. Government under Contract Number HHSM-500-2012-00008I, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

This document was prepared by The MITRE Corporation under contract with the U.S. Food and Drug Administration. The views, opinions, and findings contained in this playbook do not constitute agency guidance, policy, or recommendations or legally enforceable requirements. Following the recommendations in this Playbook does not constitute compliance with any requirements of the Federal Food, Drug, and Cosmetic Act, or any other applicable law.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

Contents

Record of Changes

Version	Date	Description of Change
0.12.04.00	September 3, 2019	Initial version submitted to FDA for MDDT qualification
0.12.04.01	October 27, 2020	Added links to MDDT qualification summary and rubric calculator and revised version note to reflect MDDT status (no changes to rubric)

Introduction

The Common Vulnerability Scoring System (CVSS) is an open standard designed to convey vulnerability severity and help determine the urgency and priority of response, which is currently maintained by the Forum of Incident Response and Security Teams (FIRST) CVSS Special Interest Group (SIG). Per Food and Drug Administration (FDA) guidance, policy and regulation, medical device manufacturers need to assess the severity of vulnerabilities as part of their risk assessment process, both during product development and as part of post-market surveillance after the product has been cleared or approved and points to CVSS as an example tool for doing this. When vulnerabilities are discovered by third party researchers, manufacturers, typically working with the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC), use CVSS to score the vulnerability as part of the vulnerability disclosure process. This highlights the value of CVSS in providing a consistent and standardized way to communicate the severity of a vulnerability between multiple parties, including the medical device manufacturer, hospitals, clinicians, patients, NCCIC, and vulnerability researchers.

Nonetheless, there are challenges in using CVSS to assess the severity of vulnerabilities in medical devices. CVSS and its associated rubric and examples were developed for enterprise information technology systems and do not adequately reflect the clinical environment and potential patient safety impacts. For example, CVSS does not provoke the consideration of the medical device design and/or clinical network environment and thus does not determine the impact of a cybersecurity vulnerability on the essential performance of a medical device, nor tie this vulnerability assessment back to the clinical environment to help evaluate potential patient safety impacts.

To address these challenges, the MITRE Corporation, under contract to FDA, developed a rubric that provides guidance for how an analyst can utilize CVSS as part of a risk assessment for a medical device. This rubric was developed in collaboration with a working group of subject matter experts across the medical device ecosystem, including FDA, medical device manufacturers, healthcare delivery organizations, security experts, and safety/risk assessment experts.

The rest of this document is an informal specification of a rubric that provides guidance for how an analyst can utilize CVSS as part of a risk assessment for a medical device.

The rubric includes:

- Customized, Healthcare Delivery Organization (HDO)-specific guidance that is not included in the original specification
- Device-specific examples
- Discussion of difficulties in (1) repeatability of the rubric and/or (2) conformance to the spirit of the original CVSS v3.0 specification

- Consideration of many perspectives that would be relevant to a medical device manufacturer or an HDO, including (1) patient safety, (2) patient/clinician privacy, and (3) cybersecurity risk from an enterprise vulnerability-management perspective.
- Visual guides (in the form of "decision trees" or "flowcharts") to simplify the process

Note for this version:

Version 0.12.04 of the rubric has been qualified as a Medical Device Development Tool (MDDT). See Relevant Documents for the qualification package which defines the MDDT Context of Use. It is still a work in progress and may be revised in the future and resubmitted to FDA. Some parts of the rubric are less complete than others. Sections of this version of the rubric contain questions and commentary that are intended to focus users to consider issues that have arisen during the production of the rubric that may help in applying it during a vulnerability assessment.

Relevant Documents

Name: Common Vulnerability Scoring System v3.0: Specification Document
Author/Publisher: FIRST
URL: https://www.first.org/cvss/specification-document

Name: Common Vulnerability Scoring System v3.0: User Guide
Author/Publisher: FIRST
URL: https://www.first.org/cvss/user-guide

Name: CVSS v3.0 Calculator
Author/Publisher: FIRST
URL: https://www.first.org/cvss/calculator/3.0

Name: Medical Device Development Tool Qualification Summary
Author/Publisher: MITRE
URL: https://www.fda.gov/media/143131/download

Name: Medical Device CVSS Rubric Calculator
Author/Publisher: MedSec
URL: https://github.com/mitre/md-cvss-rubric-tools

Organization and Use of the Rubric

The rubric is structured as a series of questions at various decision points. Each portion of the CVSS vector has its own rubric and series of structured questions. Each answer should be recorded by the analyst. Many answers provide direct suggestions for how to fill out a portion of the CVSS vector; typically, the analyst is expected to use the first vector suggestion that is associated with the question(s), as the questions are organized in a way that prioritizes answers with the most significant contribution to the CVSS score. Other questions ask for additional information that does not directly affect the CVSS vector, but the answers could be used by the manufacturer/HDO in conducting additional risk analysis. By design, the rubric can cause the analyst to “skip” some subsequent questions that become irrelevant when the analyst follows a different branch. The rubric also allows the analyst to record when an answer is unknown; the worst-case metric value is then used for the scoring engine.

Finally, when the answer to a question suggests that the vulnerability might have an adverse effect on patient safety, there is an explicit notice that the analyst might need to perform a safety-oriented hazards analysis to determine whether the issue must be reported to FDA/CDRH as covered in the Post-Market Guidance. Such items are marked as PIPS, an informal acronym that stands for “Potential Impact to Patient Safety.”

In addition to the series of structured questions, each portion of the CVSS vector has a Decision Flow diagram and an Extended Vector table. The Decision Flow diagram depicts the decision flow logic of the series of structured questions in a graphical format. The Extended Vector table specifies the extended vector that results from answering the series of structured questions: the table defines the corresponding extended vector element and its allowed values for each question.

For better results, the scoring exercise should involve consultation with a group of subject matter experts (SMEs), not just a single analyst. From the perspective of patient safety, at a minimum, the following knowledge areas should be shared across the entire group, although it is expected that each SME might only been an expert in one area:

- Cybersecurity and privacy
- Device engineering, design, and architecture
- Patient health impact from resulting hazards
- HDO device usage scenarios and clinical workflow impact
- Information technology integration and interoperability

Output of the Rubric

Once the analyst applies the rubric to a particular vulnerability or security concern for a medical device, the following information could be provided as output:

- CVSS score (between 0 and 10.0), as calculated using the FIRST CVSS v3.0 specification;
- CVSS vector (a set of tuples), as defined in the FIRST CVSS v3.0 specification;
- Answers to the rubric's related questions, which may help guide or understand healthcare-specific considerations for the larger risk analysis. Currently, these are being represented in a way that allows creation of an "extended vector" that has the same syntax as a CVSS vector; each measure's code begins with "X." An example scorecard is included in this document.

Scoring Guidance

1. The Decision Flow diagrams and the text-based question series should be used in combination. The Decision Flow diagrams provide an overview of the logical flow of the questions (which can be difficult to follow in the text-based series of questions), while the text-based series of questions should be regarded as more authoritative, providing additional guidance and examples beyond the diagrams.
2. Consult the Clarifications and Examples to ensure that you understand what the questions are asking.
3. When a question could have multiple valid answers, then choose the answer for the worst-case scenario.
4. When the answer is not known or uncertain, select "Unknown" (U) for the question, and use the recommended metric value that is associated with "Unknown." The rubric defines the recommended value in a way that maximizes the resulting score; that is, the rubric makes a conservative, worst-case assumption when the answer is unknown.
5. For each metric, the nested, branching style of the rubric may cause the analyst to effectively "skip" some subsequent questions that become irrelevant based on answers to previous questions. For completeness, the analyst can select the "Not Answered" (NA) value for questions that are skipped. This makes it explicit that the question was not accidentally omitted.
6. Identify and focus on the root cause of the problem – that is, the underlying vulnerability – and less on the attack that has been identified. Often, a single vulnerability can be subjected to multiple attacks.
7. In general, scoring is intended to be performed on the vulnerability in isolation from other factors or other related attacks or vulnerabilities. When analyzing an attack chain in the context of CVSS scoring, concentrate only on the prerequisites of the current vulnerability, and not any previously-exploited vulnerabilities. For example, consider a chain in which the adversary exploits a remote service to obtain shell access as a local unprivileged user, then – as that user - exploits a separate Elevation of Privilege (EoP) vulnerability to gain access to the OS kernel itself. When scoring the EoP vulnerability, the attacker is starting with "local" access, and not network-based.

8. When the rubric and documentation do not provide sufficient clarity, consult the associated FIRST documentation or guidance.
9. If there are multiple scenarios that may cause significant differences in scoring (such as the presence or absence of optional features), then consider scoring each scenario separately, and either aggregate the scores or choose the highest score.

=========== Base Metric Group ============

=== Attack Vector (AV) ===

Type: Exploitability

Specification: https://www.first.org/cvss/specification-document#2-1-1-Attack-Vector-AV

Q1 (XAVN). Can the attacker utilize some type of network or communication protocol to exploit this vulnerability? Note: Do NOT consider firewall or other access restrictions for this question (see "Working Group Discussion" section).

- **Yes: Q2 (XAVT). Does the network use OSI layer 3 or 4 protocols, e.g. IP, TCP/IP, or UDP?**
    - **Yes: AV = "N" (Network)**
        - Whether from the Internet or anywhere within the environment's Intranet
        - If there is any access from at least one Internet location
        - Includes access from third-party networks (e.g. manufacturer systems with access to hospital-internal network)
    - **No: Q3 (XAVW). Is the communication over a wireless channel?**
        - **Yes: Q4 (XAVR). Is the range approximately 10 feet or less?**
            - **Yes: AV = "L" (Local).** Attacker is physically close to the victim or target, and is presumed to have implied authorization, using short-range communications such as:
                - Bluetooth LE
                - Zigbee

- Inductive communication
- Near Field Communications (NFC)

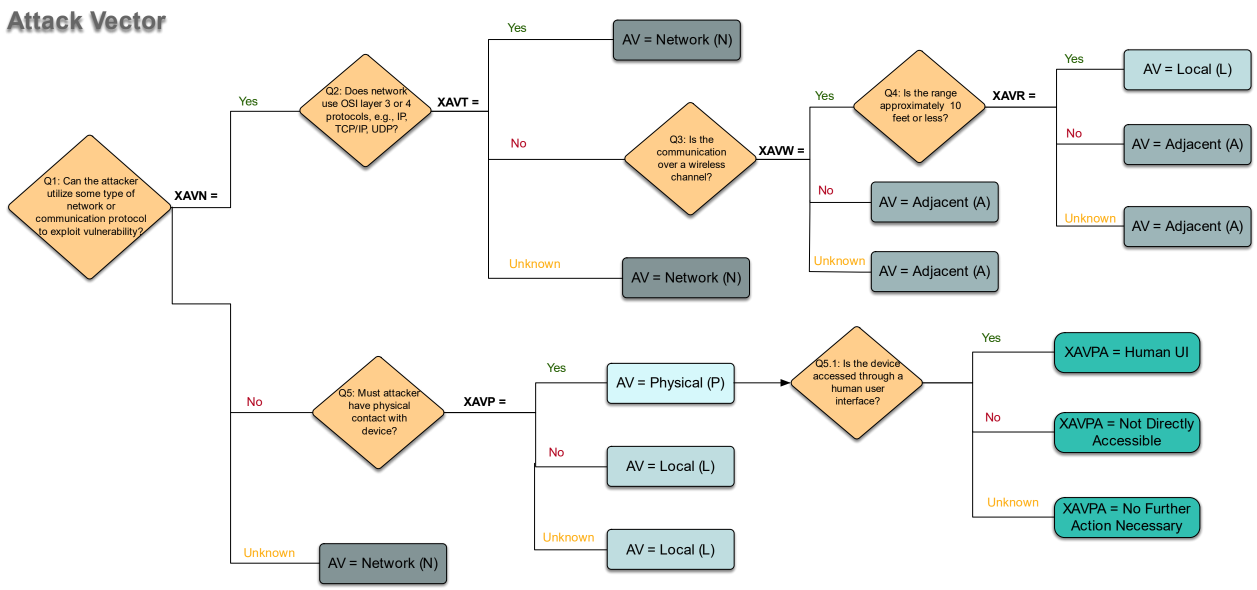
- **No: AV = “A” (Adjacent).** Attacker is on wireless channel, possibly with a relatively wide range, e.g. network across an entire physical facility or building.
  - 802.11b
  - Bluetooth
- **Unknown: AV = “A” (Adjacent).**

- **No: AV = “A” (Adjacent).** Attacker is on:
  - Same physical network
  - Same network segment
- **Unknown: AV = “A” (Adjacent).**

- **Unknown: AV = “N” (Network).**

- **No: Q5 (XAVP). Must the attacker have physical contact with the device?**
  - **Yes: AV = “P” (Physical).**
    - **Q5.1 (XAVPA). Is the device accessed through a “human-user interface,” i.e. a user interface intended for manual operation by device users?**
      - **Yes: Human UI.** An intended human user (patient, clinician, or admin) can interact with the vulnerable interface using a keyboard or mouse; GUI of a touch-screen monitor; inserting physical media such as USB, DVD, CD, or floppy disk; plugging something into a physical port, e.g. serial port; etc.
      - **No: Not Directly Accessible.** An unintended interface in which an attacker must use tools or unusual techniques to bypass a protective case or shielding; use electronics e.g. JTAG/SWD; or otherwise break through some other type of physical barrier on or within the device itself.
      - **Unknown:** No further action necessary.
  - **No: AV = “L” (Local).** Attacker has logon or shell access to the system/device
  - **Unknown: AV = “L” (Local).**
- **Unknown: AV = “N” (Network).**

Attack Vector Decision Flow


Attack Vector
Q1: Can the attacker utilize some type of network or communication protocol to exploit vulnerability?
XAVN =
Yes
Q2: Does network use OSI layer 3 or 4 protocols, e.g., IP, TCP/IP, UDP?
XAVT =
Yes
AV = Network (N)
No
Q3: Is the communication over a wireless channel?
XAVW =
Yes
Q4: Is the range approximately 10 feet or less?
XAVR =
Yes
AV = Local (L)
No
AV = Adjacent (A)
Unknown
AV = Adjacent (A)
No
AV = Adjacent (A)
Unknown
AV = Adjacent (A)
Unknown
AV = Network (N)
No
Q5: Must attacker have physical contact with device?
XAVP =
Yes
AV = Physical (P)
Q5.1: Is the device accessed through a human user interface?
Yes
XAVPA = Human UI
No
XAVPA = Not Directly Accessible
Unknown
XAVPA = No Further Action Necessary
No
AV = Local (L)
Unknown
AV = Local (L)
Unknown
AV = Network (N)

Attack Vector Extended Vector

Question	Element	Values
Q1: Can the attacker utilize some type of network or communication protocol to exploit this vulnerability?	Extended Attack Vector Network (XAVN)	Yes (Y) No (N) Unknown (U)
Q2: Does the network use OSI layer 3 or 4 protocols, e.g. IP, TCP/IP, or UDP?	Extended Attack Vector TCP/IP or UDP (XAVT)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Is the communication over a wireless channel?	Extended Attack Vector Wireless (XAVW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is the range approximately 10 feet or less?	Extended Attack Vector Range (XAVR)	Yes (Y) No (N)

		Unknown (U) Not Answered (NA)
Q5: Must the attacker have physical contact with the device?	Extended Attack Vector Physical (XAVP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5.1: Through an intended human UI?	Extended Attack Vector Physical Access Type (XAVPA)	Human UI Not Directly Accessible No Further Action Necessary

Clarifications

The “Local” vector can imply that the attacker has access to a shell or other capability that allows the attacker to launch a relatively arbitrary set of commands or programs that are available on the system. In some cases, such a shell might only be available through a remote service (such as Telnet or SSH), but after authenticating to the system, the user is “Local” to the system. Roughly speaking, there is an implication that a successful attacker can perform an “Elevation of Privilege” or is otherwise an “insider” to the system.

For purposes of Base scoring, physical access (and associated protection mechanisms) assumes a “worst case” scenario in which any person who has physical access to the device is assumed to be allowed to physically interact with the device. Protection mechanisms such as cipher-locked doors may be considered in the Modified Attack Vector (MAV), as covered in the Environmental group.

Working Group Discussion

For hospital environments that use network segmentation, firewalls, etc. that limit access to Layer 3 or 4 traffic (e.g. TCP/IP), there may be a temptation to use “Adjacent.” However, the CVSS v3.0 documentation states that the (N)etwork option also applies to the environment’s Intranet. There does not appear to be a clear way to represent such network separation. The FIRST SIG will be consulted about how to manage this issue; however, see the “Modified Attack Vector (MAV)” section in this rubric.

As such, even non-hospital networked systems - including those from trusted manufacturers - are likely to be scored as "Network," not “Adjacent.”

For the purposes of this rubric, inductive communications are regarded as "Local” because there is no physical contact with the device or patient, but possession of the inductive component and the requirement of close range implies a certain degree of “authorization.”

The range of 10 feet for wireless communications is debatable. The intention is to reflect how “close” the attacker must be, roughly within the same room or physical space. It is recognized that wireless attackers of different skills and equipment capabilities can increase their range, but this is too complicated to capture within the rubric.

=== Attack Complexity (AC) ===

Type: Exploitability

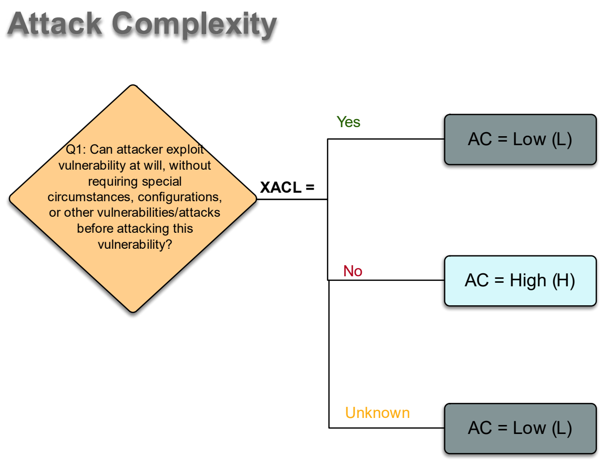
Specification: https://www.first.org/cvss/specification-document#2-1-2-Attack-Complexity-AC

Q1 (XACL). Can the attacker attempt to exploit the vulnerability at will, i.e., without requiring any special circumstances, configurations, or use of other vulnerabilities or attacks before attacking this vulnerability? Note: do not consider the types of privileges the attacker needs, or how much interaction with a victim is required, as these are covered elsewhere.

- **Yes: AC = “L” (Low).** The attacker can expect frequent, reliable success against the vulnerability, or make repeated attempts to exploit the vulnerability, with minimal effort.
- **No: AC = “H” (High).** The attacker must perform additional steps, such as
    - Obtaining sensitive information such as shared secrets
    - Rare, non-default configurations
    - Conducting a “man-in-the-middle” attack by controlling or alternating the communication channel to “spoof” a trusted host or component
    - Defeating a built-in protection mechanism or control that is intended to detect signs of attempted exploitation or make exploitation more difficult
        - Example: at the OS layer, ASLR or Data Execution Prevention
    - Conducting a series of repeated steps that each have a low or unpredictable chance of success, such as attempts to win a race condition with a very narrow

time window
  - Forcing the victim to perform a series of unusual, seemingly suspicious steps
  - Reliance on unpredictable, inadvertent user error
  - Reliance on victim's negligence
- **Unknown: AC = "L" (Low).**

Attack Complexity Decision Flow


Attack Complexity
Q1: Can attacker exploit vulnerability at will, without requiring special circumstances, configurations, or other vulnerabilities/attacks before attacking this vulnerability?
XACL =
Yes
AC = Low (L)
No
AC = High (H)
Unknown
AC = Low (L)

Attack Complexity Extended Vector

Question	Element	Values
Q1: Can the attacker exploit the vulnerability at will, i.e., without requiring any special circumstances, configurations, or use of	Extended Attack Complexity (XACL)	Yes (Y) No (N) Unknown (U)

other vulnerabilities or attacks before attacking this vulnerability?		

Clarifications

Scoring MUST NOT consider how difficult it is for the attacker to initially discover the vulnerability and figure out the steps required to exploit it. Instead, the analyst must assume that the attacker has “full knowledge” of program code, protocols and specifications, data formats, configurations, hard-coded and default passwords or keys, and other knowledge, including access to manuals for users and/or service technicians. The analyst must also assume that the attacker can obtain any automated program or exploit that encodes this knowledge.

Examples

Inadvertent user errors may already be covered within the product’s hazard analysis.

With respect to infusion pumps, some examples of unpredictable user errors include:

- The doctor accidentally enters an incorrect dosage for drug delivery due to differences in units of measurement
- A clinician accepts a drug library change without verifying that the change was expected
- A clinician incorrectly accepts an alert stating that rate of infusion is higher than maximum

For victim negligence, some examples are:

- A configuration file is installed with restrictive permissions, but the administrator sets the permissions so that the file can be modified by any regular, unprivileged user
- The attacker gives the victim a series of precise steps to follow, such as a series of commands.

Working Group Discussion

For purposes of Base scoring, physical access to a device is captured as part of the Attack Vector. However, certain types of physical attacks may be more difficult to execute than others. It is not clear how much detail is necessary to capture within the rubric to distinguish between “High” and “Low” complexity physical attacks. In addition, some protection mechanisms in the hospital may need to be considered in the Environmental portion of the rubric; for example, hospitals may have restricted areas or locked devices.

Additional Comments

For cases in which attacks require physical access, the analyst may wish to consider how much time and which physical tools are required in order to successfully perform the attack. As documented in "Attack Vector," there may be a directly accessible interface that is intended to be accessed easily, such as a keyboard or touch screen; this contrasts with physical disassembly of the device that bypasses anti-tamper capabilities and requires removal of protective plates in order to access the vulnerable component.

=== Privileges Required (PR) ===

Type: Exploitability

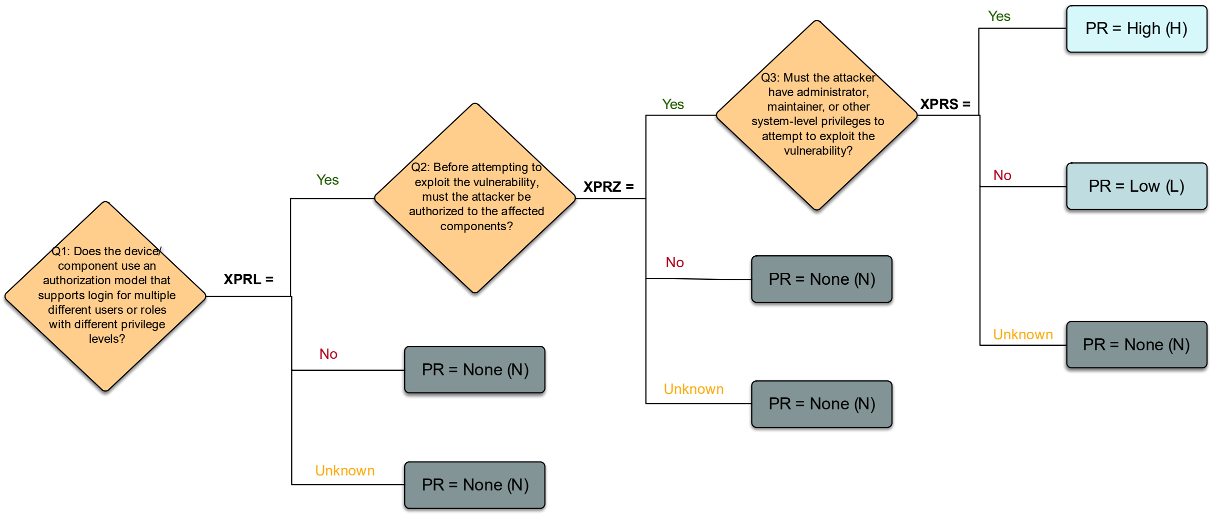
Specification: https://www.first.org/cvss/specification-document#2-1-3-Privileges-Required-PR

Q1 (XPRL). Does the device/component use an authorization model that supports login for multiple different users or roles with different privilege levels?

- **Yes: Q2 (XPRZ). Before attempting to exploit the vulnerability, must the attacker be authorized to the affected component?**
    - **Yes: Q3 (XPRS). Must the attacker have administrator, maintainer, or other system-level privileges to attempt to exploit the vulnerability?**
        - **Yes: PR = "H" (High).**
        - **No: PR = "L" (Low).**
        - **Unknown: PR = "N" (None).**
    - **No: PR = "N" (None).**
    - **Unknown: PR = "N" (None).**
- **No: PR = "N" (None).**
- **Unknown: PR = "N" (None)**

Privileges Required Decision Flow

Privileges Required


Q1: Does the device/ component use an authorization model that supports login for multiple different users or roles with different privilege levels?
XPRL =
Yes
Q2: Before attempting to exploit the vulnerability, must the attacker be authorized to the affected components?
No
PR = None (N)
Unknown
PR = None (N)
XPRZ =
Yes
Q3: Must the attacker have administrator, maintainer, or other system-level privileges to attempt to exploit the vulnerability?
No
PR = None (N)
Unknown
PR = None (N)
XPRS =
Yes
PR = High (H)
No
PR = Low (L)
Unknown
PR = None (N)

Privileges Required Extended Vector

Question	Element	Values
Q1 Does the device/component use an authorization model that supports login for multiple different users or roles with different privilege levels?	Extended Privileges Required Low (XPRL)	Yes (Y) No (N) Unknown (U)
Q2: Before attempting to exploit the vulnerability, must the attacker be authorized to the affected component?	Extended Privileges Required Authorization (XPRZ)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Must the attacker have administrator, maintainer, or other system-level privileges to attempt to exploit the vulnerability?	Extended Privileges Required System-Level (XPRS)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Some devices - especially legacy devices - do not support multiple users and/or roles; anybody with access to the device is effectively treated the same. If there is only one "user" or "role," then it is assumed that the "user" does not require any special privileges, and PR is ultimately set to None.

For purposes of scoring, this is focused only on the authorization model(s) that the device offers; if physical access is required, that is already covered in Attack Vector (AV).

=== User Interaction (UI) ===

Type: Exploitability

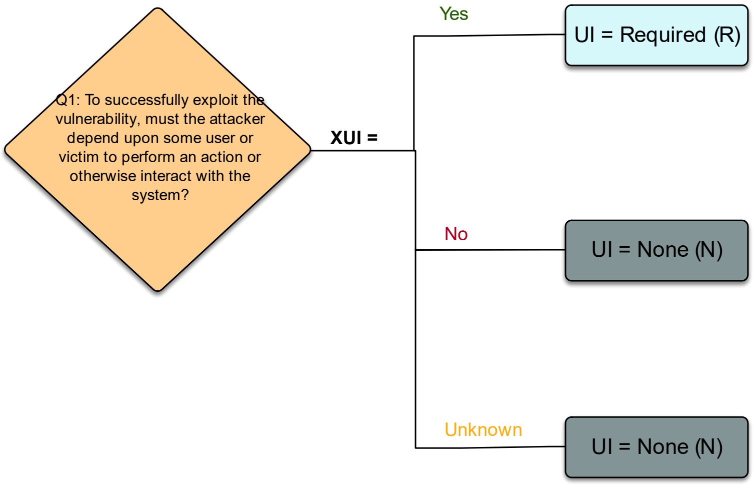
Specification: https://www.first.org/cvss/specification-document#2-1-4-User-Interaction-UI

Q1 (XUI). To successfully exploit the vulnerability, must the attacker depend on another user or victim to perform an action or otherwise interact with the system?

- **Yes: UI = "R" (Required).**
- **No: UI = "N" (None).**
- **Unknown: UI = "N" (None).**

User Interaction Decision Flow

User Interaction


Q1: To successfully exploit the vulnerability, must the attacker depend upon some user or victim to perform an action or otherwise interact with the system?
XUI =
Yes
UI = Required (R)
No
UI = None (N)
Unknown
UI = None (N)

User Interaction Extended Vector

Question	Element	Values
Q1: To successfully exploit the vulnerability, must the attacker depend on some user or victim to perform an action or otherwise interact with the system?	Extended User Interaction (XUI)	Yes (Y) No (N) Unknown (U)

Clarifications

The user/victim must be a separate individual who is not the attacker. (That is, it is assumed that attackers do not gain any extra benefit from only attacking themselves.)

Examples

For infusion pumps, some scenarios are:

- A vulnerability allows modification of a drug library, but the clinician has to manually approve the library change using a dialog on the device itself.
- A vulnerability allows code execution by causing a long log entry to be created, but the vulnerability can only be exploited if the device's administrator inserts a USB drive and chooses to export the log files to the USB drive.

=== Scope (S) ===

Type: Impact

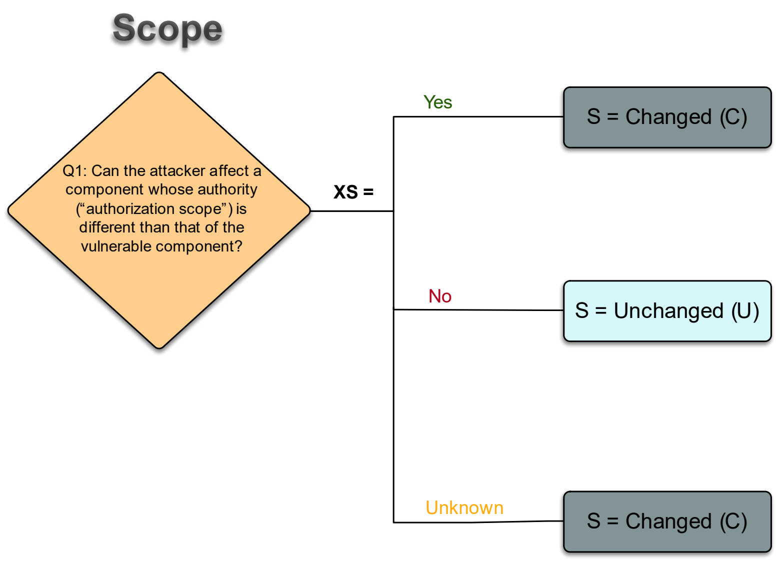
Specification: https://www.first.org/cvss/specification-document#2-2-Scope-S

User Documentation: https://www.first.org/cvss/user-guide#2-1-Scope-Vulnerable-Component-and-Impacted-Component

Q1 (XS). Can the attacker affect a component whose authority ("authorization scope") is different than that of the vulnerable component?

- **Yes: S = "C" (Changed).** The effect of the attack extends beyond the affected component, such as:
  - Sandbox
  - Virtual machine host operating system
  - Other systems or devices that depend on information or functionality from the vulnerable component in order to provide Essential Performance
  - Other systems or devices to which the vulnerable device connects
- **No: S = "U" (Unchanged).**
- **Unknown: S = "C" (Changed).**

Scope Decision Flow


Scope
Q1: Can the attacker affect a component whose authority ("authorization scope") is different than that of the vulnerable component?
XS =
Yes
S = Changed (C)
No
S = Unchanged (U)
Unknown
S = Changed (C)

Scope Extended Vector

Question	Element	Values
Q1: Can the attacker affect a component whose authority ("authorization scope") is different than that of the vulnerable component?	Extended Scope (XS)	Yes (Y) No (N) Unknown (U)

Working Group Discussion

In working-group telecons and the pilot testing program in February 2019, it was difficult to discuss this metric and its potential implications. Perhaps it is too dependent on specific scenarios or device classes. There also needs to be guidance about the level of detail to which one would consider if there is a different authorization scope; e.g., in an embedded device, the chip set might technically involve a different authorization scope than the microprocessor, but this distinction might be too precise. Further investigation is needed. Additional healthcare-specific examples will be useful.

Clarifications

As of April 2019, the CVSS SIG has been working on changes to the specification and user documentation to further clarify how a Scope change is defined. Many of these changes appear likely to be integrated into a new CVSS 3.1 version.

There can be significant disagreement as to whether a Scope change can occur or not, partially stemming from disagreements among people regarding what the definition of a Scope change really is. The specification and user documentation for CVSS 3.0 should be consulted carefully when performing scope analysis.

- Since "component" is a general term, analysts for a particular vulnerability should ensure that they agree about what constitutes a "component." For example, a single physical medical device might consist of multiple smaller components, but the physical device might also be regarded as a component within a larger system-of-systems that includes other devices or network components.
- Two components are considered: the vulnerable component that contains the vulnerability, and the impacted component whose confidentiality, integrity, and/or availability is directly affected by exploitation of the vulnerability. In many cases, the vulnerable component and the impacted component are the same, and there is no scope change.
- The emphasis of the analysis is on whether two components have a different "Authority" or "authorization scope."
- When both the vulnerable component and impacted component are affected, the analyst should assess the CIA impact that is most severe.
- When the vulnerable component is part of a system of systems, and the vulnerable component has significant control over the operation of other components within this system-of-systems, then these impacted systems likely constitute a scope change. For example, if a clinician programmer contains a vulnerability that allows attackers to cause the programmer to download malicious firmware onto an implanted device, then this is considered a scope change. As another example, if a router contains a vulnerability that allows an attacker to modify the ARP table, then there is a scope change, since the ARP table is directly used to support communications with services on other systems being internetworked through the router.

Examples

Consider the following scenarios, which may help to clarify when Scope should be marked as Changed or Unchanged:

- A virtual machine has a different authority than the host operating system. Compromise of a virtual machine should not have any impact on the host OS. If an attack against the virtual machine can be used to gain privileges to the host operating system, then the Scope would be Changed.
- In CVSS SIG discussions for possible CVSS 3.1 changes, cross-site scripting (XSS) is typically considered to involve a scope change, since the vulnerable component is typically the web server (whose Authority is from the service provider) is different than the impacted component (the web browser, whose authority is from the individual user / operating system that is running the browser). However, attacks such as SQL injection typically do NOT involve a scope change, since the affected web application runs under the same authorization scope / authority as the SQL database server.
- Consider a clinician programmer that is used to reprogram a medical device that is self-contained, mobile, and attached to the patient's body independently of the programmer, such as an insulin pump or a pacemaker. If a vulnerability in the programmer allows an attacker to cause the medical device to be updated with malicious firmware, then there is a scope change.
- Consider a home monitor for an on-person medical device such as a pacemaker or CPAP machine. Suppose that this monitor is only intended to periodically read data from the medical device, then transmit this data to a hospital's network, where the data can be analyzed by doctors. If a vulnerability in the home monitor can be used to modify the data before it is sent to the hospital, then this does NOT indicate a scope change – the data is not modified on the medical devices themselves, and the only impacted component is the home monitor. However, suppose the monitor contains extra code and physical components that could be used to reprogram the medical device (e.g., the home monitor happens to have the same library that is shared with clinician programmers to minimize manufacturer's maintenance costs). A vulnerability in the home monitor that allows reprogramming of the medical devices would cause the scope to be changed.

=== Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A) ===

Type: Impact

Specifications:

- https://www.first.org/cvss/specification-document#2-3-1-Confidentiality-Impact-C
- https://www.first.org/cvss/specification-document#2-3-2-Integrity-Impact-I
- https://www.first.org/cvss/specification-document#2-3-3-Availability-Impact-A

CVSS has individual vector elements in the Base Metric Group that characterize the technical impacts on confidentiality, integrity, and availability if the vulnerability is exploited. This section of the rubric provides guidance in scoring the CIA vector elements through a systematic consideration of the different types of data and processes which potentially can be impacted by the vulnerability. For each type of data/functionality, the analyst should consider if exploitation of the vulnerability enables the attacker to read, modify/delete, or prevent access to that data/functionality. Although the analysis is combined, at the end individual CVSS vector elements and extended vector elements will be generated for confidentiality, integrity, and availability impacts.

Action 1. For each type of data or functionality that may be considered sensitive, restricted, or important by the HDO, patients, clinicians, or other caretakers, determine if the attacker can read, modify/delete, or prevent access to that data or functionality. For each type of data or functionality that can be read, modified/deleted, or made inaccessible, consider the impact if an attacker is able to read, modify/delete, or prevent access to that data or functionality. For each type of data listed, identify whether the impact is High, Low, or None. If a given type of data is not supported, use None. Answer every question.

- **For any PHI/PII data:**
    - **Q1.C (XCP): Can this data be read?**
        - **No: XCP = None.** Go to next question
        - **Yes: XCP = High.**
        - **Q1.1.C (XCPM): Can the exposed data cover a large number of patients, e.g. 500 or more, which may force regulatory action or data breach notification (e.g. HIPAA, GDPR)*?*** Go to next question.
            - **Yes: XCPM = "Y" (Yes).** Consider breach notification and other regulatory requirements.
            - **No: XCPM = "N" (No).**
            - **Unknown: XCPM = "U" (Unknown).**
        - **Unknown:** It is unknown if there is any PHI/PII affected. Go to next question.
        - Note: Do not use Low for this question because a privacy breach is binary (it happened or didn't happen).
    - **Q1.I (XIP): Can this data be modified/deleted? (XIP = High/Low/None/Unknown). PIPS.** Go to next question.
        - **High:** the PHI/PII may be modified to reference other consumers or delete/remove individual details associated with a single consumer
        - **Low:** PHI/PII can be affected, but the associated consumer's identity cannot be changed, and records cannot be deleted
        - **Unknown:** It is unknown if there is any PHI/PII affected.
    - **Q1.A (XAP): Can this data be rendered inaccessible? (XAP = High/Low/None/Unknown). PIPS.** Go to next question.
        - **High:** PHI/PII that is critical to the consumer's identity, and/or is used as an important ID or primary key within the HDO's information systems
        - **Low:** other, non-critical PHI/PII
        - **Unknown:** It is unknown if there is any PHI/PII affected
- **For any data or functionality related to diagnosis or monitoring:**
    - **Q2.C (XCD): Can this data or functionality be read/exposed? (XCD = High/Low/None/Unknown).** Go to next question.

        - **High:** some data provides specific details related to diagnosis/monitoring, e.g. physiological readings or lab results
        - **Low:** only metadata or summarized data is exposed (e.g. timestamps)
        - **Unknown:** It is unknown whether any diagnosis/monitoring data is affected; or, the impact to diagnosis or monitoring cannot be decided
    - **Q2.I (XID): Can this data or functionality be modified/deleted? (XID = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** modified data includes specific details related to diagnosis/monitoring, e.g. physiological readings or lab results
        - **Low:** only metadata or summarized data can be modified (e.g. timestamps)
        - **Unknown:** It is unknown whether any diagnosis/monitoring data is affected; or, the impact to diagnosis or monitoring cannot be decided
    - **Q2.A (XAD): Can this data or functionality be rendered inaccessible? (XAD = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** clinicians cannot obtain specific details essential for diagnosis/monitoring, e.g. physiological readings or lab results
        - **Low:** only metadata or summarized data cannot be accessed (e.g. timestamps)
        - **Unknown:** It is unknown whether any diagnosis/monitoring data is affected; or, the impact to diagnosis or monitoring cannot be decided
- **For any data or functionality related to the delivery of therapy:**
    - **Q3.C (XCT): Can this data or functionality be read/exposed? (XCT = High/Low/None/Unknown).** Go to next question.
        - **High:** some data provides specific details related to the delivery of therapy (e.g., drug, dosage, infusion rate, radiation plan)
        - **Low:** only metadata or summarized data is exposed (e.g. timestamps)
        - **Unknown:** It is unknown whether therapy delivery is exposed; or the impact to delivery of therapy cannot be decided
    - **Q3.I (XIT): Can this data or functionality be modified/deleted? (XIT = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** the modified data can be used to modify, prevent, or significantly delay delivery of therapy (e.g. for "modify": change dose, change rate, change physical area to be covered by radiation, etc.)
        - **Low:** the modified data can be used for minor, non-clinically-important delays of therapy, and/or introduce inconvenience to clinicians
        - **Unknown:** It is unknown whether therapy delivery is affected; or the impact to delivery of therapy cannot be decided
    - **Q3.A (XAT): Can this data or functionality be rendered inaccessible? (XAT = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** inability to access the data can interfere with, prevent, or significantly delay delivery of therapy (e.g. for "interfere with": unable to change dose, change rate, change physical area to be covered by radiation, etc.)

        - **Low:** inability to access the data can cause minor, non-clinically-important delays of therapy, and/or introduce inconvenience to clinicians
        - **Unknown:** It is unknown whether therapy delivery is affected; or, the impact to delivery of therapy cannot be decided
- **For any data or functionality related to clinical workflow:**
    - **Q4.C (XCW): Can this data or functionality be read/exposed? (XCW = High/Low/None/Unknown).** Go to next question.
        - **High:** private or proprietary details about clinical workflow, clinicians, etc. can be obtained
        - **Low:** non-private details about workflow or clinicians can be obtained
        - **Unknown:** it is unknown whether any data related to clinical workflow is exposed; or, the impact to workflow cannot be decided
    - **Q4.I (XIW): Can this data or functionality be modified/deleted? (XIW = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** private or proprietary details about clinical workflow, clinicians, etc. can be modified or deleted
        - **Low:** non-private details about workflow or clinicians can be modified or deleted
        - **Unknown:** it is unknown whether any data related to clinical workflow is affected; or, the impact to workflow cannot be decided
    - **Q4.A (XAW): Can this data or functionality be rendered inaccessible? (XAW = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** inability to access the data can cause significant disruption or inefficiencies to clinical workflow
        - **Low:** inability to access the data can cause slight inefficiencies or clinician inconvenience to clinical workflow
        - **Unknown:** it is unknown whether any data related to clinical workflow is affected; or, the impact to workflow cannot be decided
- **For any data or functionality related to private system or system-user data, e.g. passwords or private keys:**
    - **Q5.C (XCS): Can this data or functionality be read/exposed? (XCS = High/Low/None/Unknown).** **PIPS.** Go to next question.
        - **High:** the system or system-user data is critical to the proper operation of the system, e.g. passwords or private keys
        - **Low:** the system or system-user data is only related to limited functionality regarding operation of the system; knowledge of this data by attackers should be disallowed, but does not interfere with proper operation of the system
        - **Unknown:** it is unknown whether any system/system-user data is exposed; or, the impact cannot be decided
    - **Q5.I (XIS): Can this data or functionality be modified/deleted? (XIS = High/Low/None/Unknown).** **PIPS.** Go to next question.

        - **High:** the system or system-user data is critical to the proper operation of the system, e.g. passwords or private keys
        - **Low:** the system or system-user data is only related to limited functionality regarding operation of the system; modification of this data by attackers should be disallowed, but it does not interfere with proper operation of the system
        - **Unknown:** it is unknown whether any system/system-user data is affected; or, the impact cannot be decided
    - **Q5.A (XAS): Can this data or functionality be rendered inaccessible? (XAS = High/Low/None/Unknown).** PIPS. Go to next question.
        - **High:** inability to access the system or system-user data prevents or disrupts the proper operation of the system
        - **Low:** inability to access the system or system-user data only prevents or disrupts the operation of non-critical portions of the system
        - **Unknown:** it is unknown whether any system/system-user data is affected; or, the impact cannot be decided
- **For any other kind of critical, sensitive data or functionality:**
    - **Q6.C (XCO): Can this data or functionality be read/exposed? (XCO= High/Low/None/Unknown).** Go to next question.
    - **Q6.I (XIO): Can this data or functionality be modified/deleted? (XIO = High/Low/None/Unknown).** PIPS. Go to next question.
    - **Q6.A (XAO): Can this data or functionality be rendered inaccessible? (XAO = High/Low/None/Unknown).** PIPS. Go to next question.

Q7 (XCH): Is “High” or “Unknown” the answer for at least one of Q1.C through Q6.C?

- **Yes: C = “H” (High)**.
- **No: Q8 (XCL). Is “Low” the answer for at least one of Q1.C through Q6.C?**
    - **Yes: C = “L” (Low).**
    - **No: C = “N” (None).**

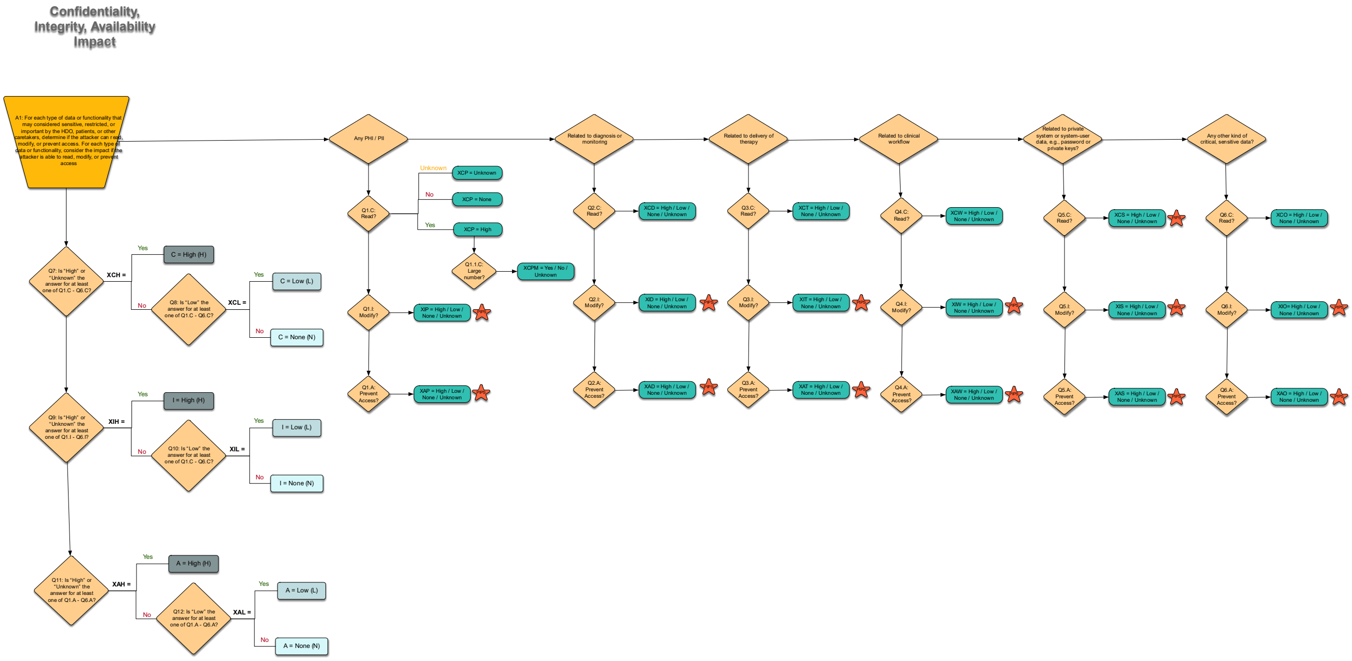
Q9 (XIH): Is “High” or “Unknown” the answer for at least one of Q1.I through Q6.I?

- **Yes: I = “H” (High)**.
- **No: Q10 (XIL). Is “Low” the answer for at least one of Q1.I through Q6.I?**
    - **Yes: I = “L” (Low).**
    - **No: I = “N” (None).**

Q11 (XAH): Is “High” or “Unknown” the answer for at least one of Q1.A through Q6.A?

- **Yes: A = “H” (High)**.
- **No: Q12 (XAL). Is “Low” the answer for at least one of Q1.A through Q6.A?**
    - **Yes: A = “L” (Low).**
    - **No: A = “N” (None).**

Confidentiality, Integrity, Availability Impact Decision Flow


Confidentiality, Integrity, Availability Impact
A1: For each type of data or functionality that may considered sensitive, restricted, or important by the HDO, patients, or other caretakers, determine if the attacker can read, modify, or prevent access. For each type of data or functionality, consider the impact if the attacker is able to read, modify, or prevent access
Any PHI / PII
Q1.C: Read?
Unknown
XCP = Unknown
No
XCP = None
Yes
XCP = High
Q1.1.C: Large number?
XCPM = Yes / No / Unknown
Q1.I: Modify?
XIP = High / Low / None / Unknown
PIPS
Q1.A: Prevent Access?
XAP = High / Low / None / Unknown
PIPS
Related to diagnosis or monitoring
Q2.C: Read?
XCD = High / Low / None / Unknown
Q2.I: Modify?
XID = High / Low / None / Unknown
PIPS
Q2.A: Prevent Access?
XAD = High / Low / None / Unknown
PIPS
Related to delivery of therapy
Q3.C: Read?
XCT = High / Low / None / Unknown
Q3.I: Modify?
XIT = High / Low / None / Unknown
PIPS
Q3.A: Prevent Access?
XAT = High / Low / None / Unknown
PIPS
Related to clinical workflow
Q4.C: Read?
XCW = High / Low / None / Unknown
Q4.I: Modify?
XIW = High / Low / None / Unknown
PIPS
Q4.A: Prevent Access?
XAW = High / Low / None / Unknown
PIPS
Related to private system or system-user data, e.g., password or private keys?
Q5.C: Read?
XCS = High / Low / None / Unknown
PIPS
Q5.I: Modify?
XIS = High / Low / None / Unknown
PIPS
Q5.A: Prevent Access?
XAS = High / Low / None / Unknown
PIPS
Any other kind of critical, sensitive data?
Q6.C: Read?
XCO = High / Low / None / Unknown
Q6.I: Modify?
XIO= High / Low / None / Unknown
PIPS
Q6.A: Prevent Access?
XAO = High / Low / None / Unknown
PIPS
Q7: Is "High" or "Unknown" the answer for at least one of Q1.C - Q6.C?
XCH =
Yes
C = High (H)
No
Q8: Is "Low" the answer for at least one of Q1.C - Q6.C?
XCL =
Yes
C = Low (L)
No
C = None (N)
Q9: Is "High" or "Unknown" the answer for at least one of Q1.I - Q6.I?
XIH =
Yes
I = High (H)
No
Q10: Is "Low" the answer for at least one of Q1.C - Q6.C?
XIL =
Yes
I = Low (L)
No
I = None (N)
Q11: Is "High" or "Unknown" the answer for at least one of Q1.A - Q6.A?
XAH =
Yes
A = High (H)
No
Q12: Is "Low" the answer for at least one of Q1.A - Q6.A?
XAL =
Yes
A = Low (L)
No
A = None (N)

Confidentiality, Integrity, Availability Impact Extended Vector

Question	Element	Values
Q1 - For any PHI or PII data, can the attacker:		
Q1.C: Read PHI/PII	Extended Confidentiality PHI or PII (XCP)	High (H) Low (L) None (N) Unknown (U)

Q1.1.C: Read PHI/PII data that affects many customers	Extended Confidentiality PHI or PII – Many Customers (XCPM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q1.I: Modify PHI/PII	Extended Integrity PHI or PII (XIP)	High (H) Low (L) None (N) Unknown (U)
Q1.A: Prevent Access to PHI/PII	Extended Availability PHI or PII (XAP)	High (H) Low (L) None (N) Unknown (U)
Q2 - For any Diagnostics/Monitoring data, can the attacker:		
Q2.C: Read Diagnostics/Monitoring data	Extended Confidentiality Diagnosis or Monitoring (XCD)	High (H) Low (L) None (N) Unknown (U)
Q2.I: Modify Diagnostics/Monitoring data	Extended Integrity Diagnosis or Monitoring (XID)	High (H) Low (L) None (N) Unknown (U)
Q2.A: Prevent Access to Diagnostics/Monitoring data	Extended Availability Diagnosis or Monitoring (XAD)	High (H) Low (L) None (N) Unknown (U)
Q3 - For any Therapy Delivery data, can the attacker:		
Q3.C: Read Therapy Delivery Data	Extended Confidentiality Therapy (XCT)	High (H) Low (L)

		None (N) Unknown (U)
Q3.I: Modify Therapy Delivery Data	Extended Integrity Therapy (XIT)	High (H) Low (L) None (N) Unknown (U)
Q3.A: Prevent Access to Therapy Delivery Data	Extended Availability Therapy (XAT)	High (H) Low (L) None (N) Unknown (U)
Q4 - For any Clinical Workflow data, can the attacker:		
Q4.C: Read Clinical workflow data	Extended Confidentiality Workflow (XCW)	High (H) Low (L) None (N) Unknown (U)
Q4.I: Modify Clinical workflow data	Extended Integrity Workflow (XIW)	High (H) Low (L) None (N) Unknown (U)
Q4.A: Prevent Access to Clinical workflow data	Extended Availability Workflow (XAW)	High (H) Low (L) None (N) Unknown (U)
Q5 - For any System/System-user data, can the attacker:		
Q5.C: Read System/System-user data	Extended Confidentiality System or System-User (XCS)	High (H) Low (L) None (N)

		Unknown (U)
Q5.I: Modify System/System-user data	Extended Integrity System or System-User (XIS)	High (H) Low (L) None (N) Unknown (U)
Q5.A: Prevent Access to System/System-user data	Extended Availability System or System-User (XAS)	High (H) Low (L) None (N) Unknown (U)
Q6 - For any other critical/sensitive data, can the attacker:		
Q6.C: Read Other critical/sensitive data	Extended Confidentiality Other (XCO)	High (H) Low (L) None (N) Unknown (U)
Q6.I: Modify Other critical/sensitive data	Extended Integrity Other (XIO)	High (H) Low (L) None (N) Unknown (U)
Q6.A: Prevent Access to Other critical/sensitive data	Extended Availability Other (XAO)	High (H) Low (L) None (N) Unknown (U)
Q7: Is “High” or “Unknown” the answer for at least one of Q1.C through Q6.C?	Extended Confidentiality High (XCH)	Yes (Y) No (N)
Q8: Is “Low” the answer for at least one of Q1.C through Q6.C?	Extended Confidentiality Low (XCL)	Yes (Y) No (N)

		Not Answered (NA)
Q9: Is “High” or “Unknown” the answer for at least one of Q1.I through Q6.I?	Extended Integrity High (XIH)	Yes (Y) No (N)
Q10: Is “Low” the answer for at least one of Q1.I through Q6.I?	Extended Integrity Low (XIL)	Yes (Y) No (N)
Q11: Is “High” or “Unknown” the answer for at least one of Q1.A through Q6.A?	Extended Availability High (XAH)	Yes (Y) No (N)
Q12: Is “Low” the answer for at least one of Q1.A through Q6.A?	Extended Availability Low (XAL)	Yes (Y) No (N) Not Answered (NA)

Working Group Discussion

The Confidentiality Impact (C) measure considers whether many consumers are affected, in consideration of the regulatory requirements for large breaches (see Q1.1.C, XCPM), by attempting to capture regulations that may impose separate penalties if too many consumers are affected, e.g. 500 consumers in HIPAA. This was treated as an important consideration for prioritization by manufacturers and HDOs, even if it is outside the scope of FDA regulations with respect to patient safety. While there are no clear equivalents for integrity, it seems likely that manufacturers or HDOs would prioritize large-scale, multi-consumer data modification over modification of data for individual consumers. This will require working-group review.

In certain HDO scenarios, the ability to read data such as PII or clinical workflow could be used by an adversary to perform another attack that has an adverse impact on patient safety, e.g. knowing when and where a particular procedure is being scheduled. It is not clear how to handle these “indirect effects” to patient safety.

Currently, the rubric does not directly identify data that may be related to safety functionality, such as emergency-stop signals, alarms, or libraries with minimum/maximum dosage settings. Presumably, an adverse impact on such data is already strongly associated with an impact on therapy delivery, diagnostics, or monitoring. It might be important for the rubric to explicitly call out this type of data, and provide clarification on different considerations on confidentiality, integrity, and availability impacts.

Diagnosis and monitoring are combined into a single question (Q2) to distinguish them from delivery of therapy (Q3). It is not clear whether the rubric should split diagnosis and monitoring into separate questions, which would enable more precise information in the extended vector, but at some cost of additional complexity for the rubric itself.

Clarifications

When the Scope analysis reveals that there is at least one impacted component that is not the same as the vulnerable component, then the analyst should conduct the Confidentiality/Integrity/Availability analysis for all components, then choose the impact that is most severe.

Integrity

The ability to modify certain PII/PHI, diagnosis/monitoring data, and/or clinical workflow data could lead to delayed or incorrect therapy, so each item is labeled as PIPS.

Availability

Preventing access to PHI, diagnostic, or monitoring data could lead to delayed or incorrect therapy, so it is considered PIPS. For example, lack of access to MRI and CT scans may delay diagnoses or treatment decisions, while lack of bedside monitoring data may require workflow changes to manually collect vital signs.

In some cases, minor inconveniences or short delays in workflow may not have any adverse effect, and the clinical usage must be considered closely. For example, if a vulnerability prevents a doctor from accessing a device's recent event history for 5 seconds, then this might have zero to no impact on the resulting diagnosis; on the other hand, in an emergency room setting, a workflow delay of one minute may be fatal.

Examples

Integrity

For infusion pumps:

- If a drug library can be modified to change safety parameters such as minimum or maximum dosage, this could allow simple data-entry errors to have safety impacts by over- or under-delivering medication without triggering a safety warning.
- Modification of a patient's ID may cause confusion amongst clinicians or cause the wrong treatment to be administered if the patient's ID is replaced with that of another patient.
- If a patient's insulin pump delivers health records to a central server on a daily basis, but a vulnerability allows those records to be destroyed, then it could make root-cause diagnosis of a hypoglycemia episode difficult or impossible, delaying proper treatment.

Availability

Consider a pacemaker that interfaces with a home monitor that sends data to a central server at the HDO for later review by the patient's doctor. A vulnerability that prevents data from being sent to the server could prevent the doctor from detecting unexpected heart rhythms.

=========== Temporal Metric Group ============

=== Exploit Code Maturity (E) ===

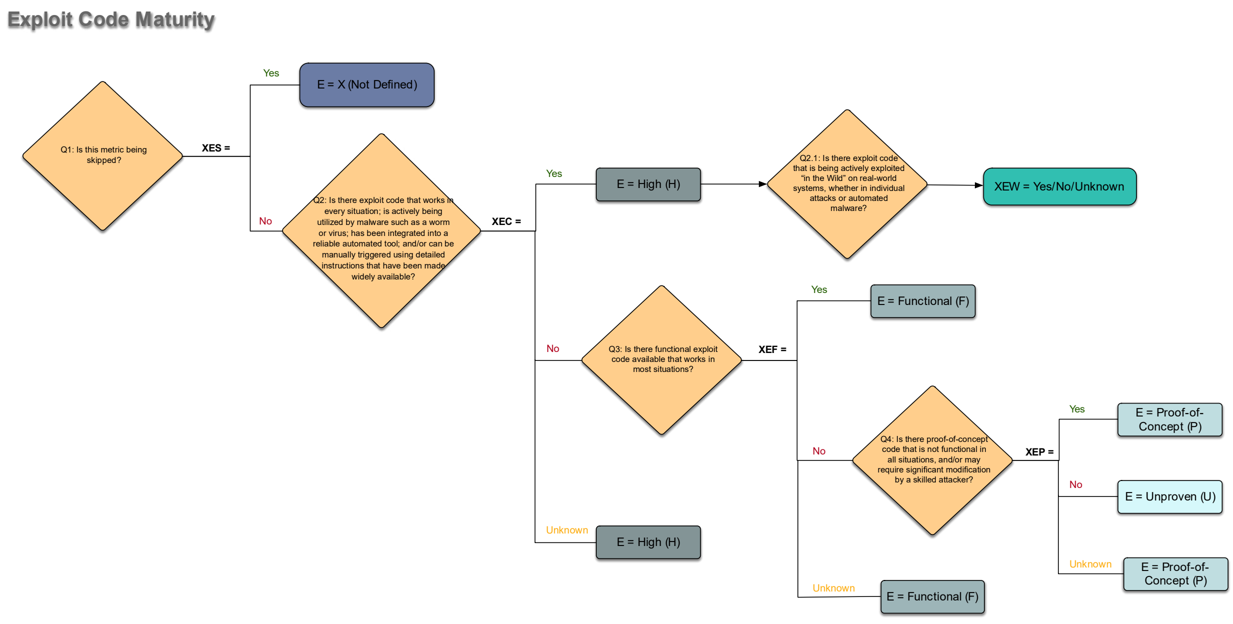
Type: Exploitability/Temporal

Specification: https://www.first.org/cvss/specification-document#3-1-Exploit-Code-Maturity-E

Q1 (XES): Is this metric being skipped?

- **Yes: set E=”X”.** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XEC): Is there exploit code that works in every situation; is actively being utilized by malware such as a worm or virus; has been integrated into a reliable automated tool; and/or can be manually triggered using detailed instructions that have been made widely available?**
  - **Yes: E=”H” (High).**
    - **Q2.1 (XEW): Is there exploit code that is being actively exploited “in the Wild” on real-world systems, whether in individual attacks or automated malware?** Answer Yes/No/Unknown.
  - **No: Q3 (XEF): Is there functional exploit code available that works in most situations?**
    - **Yes: E=”F” (Functional).**
    - **No: Q4 (XEP): Is there proof-of-concept code that is not functional in all situations, and/or may require significant modification by a skilled attacker?**
      - **Yes: E=”P” (Proof-of-Concept).**
      - **No: E=”U” (Unproven).** No exploit is known.
      - **Unknown: E=”P” (Proof-of-Concept).**
    - **Unknown: E=”F” (Functional).**
  - **Unknown: E=”H” (High).**

Exploit Code Decision Flow


Exploit Code Maturity
Q1: Is this metric being skipped?
XES =
Yes
E = X (Not Defined)
No
Q2: Is there exploit code that works in every situation; is actively being utilized by malware such as a worm or virus; has been integrated into a reliable automated tool; and/or can be manually triggered using detailed instructions that have been made widely available?
XEC =
Yes
E = High (H)
Q2.1: Is there exploit code that is being actively exploited "in the Wild" on real-world systems, whether in individual attacks or automated malware?
XEW = Yes/No/Unknown
No
Q3: Is there functional exploit code available that works in most situations?
XEF =
Yes
E = Functional (F)
No
Q4: Is there proof-of-concept code that is not functional in all situations, and/or may require significant modification by a skilled attacker?
XEP =
Yes
E = Proof-of-Concept (P)
No
E = Unproven (U)
Unknown
E = Proof-of-Concept (P)
Unknown
E = Functional (F)
Unknown
E = High (H)

Exploit Code Maturity Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Exploit Code Maturity Skipped (XES)	Yes (Y) No (N)
Q2: Is there exploit code that works in every situation; is actively being utilized by malware such as a worm or virus; has been integrated into a reliable automated tool; and/or can be manually triggered using detailed instructions that have been made widely available?	Extended Exploit Code Maturity Working Code (XEC)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q2.1: Is there exploit code that is being actively exploited "in the Wild" on real-world systems, whether in individual attacks or automated malware?	Extended Exploit Code Maturity in the Wild (XEW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Q3: Is there functional exploit code available that works in most situations?	Extended Exploit Code Maturity Functional (XEF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is there proof-of-concept code that is not functional in all situations, and/or may require significant modification by a skilled attacker?	Extended Exploit Code Maturity Proof-of-Concept (XEP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Working Group Discussion

This could consider active exploitation in targeted or untargeted attacks, whether by rapidly-spreading malware or individuals. The FIRST CVSS v3.0 specification does not directly support representing this information.

Some manufacturers, HDOs, and security consultants can make conservative assumptions about exploit maturity, e.g., the discovery of a partially-functional proof-of-concept might be assumed to be sufficient proof that a fully-functional exploit is possible. It is not clear whether (and how) this consideration should be captured by the rubric. The FIRST CVSS v3.0 specification does not directly support this conservative assumption.

=== Remediation Level (RL) ===

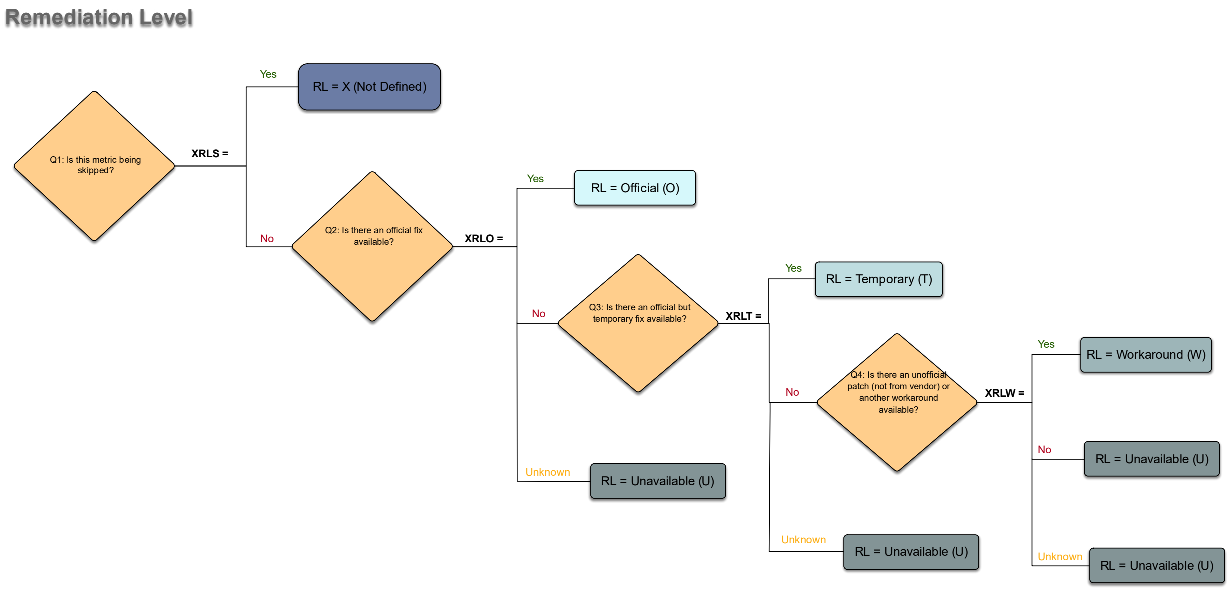
Type: Exploitability/Temporal

Specification: https://www.first.org/cvss/specification-document#3-2-Remediation-Level-RL

Q1 (XRLS). Is this metric being skipped?

- **Yes: Set RL=”X”.** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XRLO): Is there an official fix available?**
  - **Yes: RL=”O” (Official).**
  - **No: Q3 (XRLT): Is there an official but temporary fix available?**
    - **Yes: RL=”T” (Temporary).**
    - **No: Q4 (XRLW): Is there an unofficial patch (not from vendor) or another workaround available?**
      - **Yes: RL=”W” (Workaround).**
      - **No: RL=”U” (Unavailable).** No solution is available.
      - **Unknown: RL=”U” (Unavailable).**
    - **Unknown: RL=”U” (Unavailable).**
  - **Unknown: RL=”U” (Unavailable).**

Remediation Level Decision Flow



Remediation Level Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Remediation Level Skipped (XRLS)	Yes (Y) No (N)
Q2: Is there an official fix available?	Extended Remediation Level Official Mitigation (XRLO)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Is there an official but temporary fix available?	Extended Remediation Level Temporary Mitigation (XRLT)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is there an unofficial patch (not from vendor) or another workaround available?	Extended Remediation Level Workaround (XRLW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Working Group Discussion

Even if an official patch is available, HDOs may have different reasons for not deploying the patch in a timely fashion. The FIRST CVSS v3.0 specification does not support representing how "an official fix is available, but is not being used." The rubric could be extended to allow HDOs to represent alternate choices, e.g. if a Workaround or Temporary Fix can be deployed; however, such modification is probably not supported by CVSS v3.0, since the Environment group only supports "Modified Base Metrics" – not temporal.

In some likely-rare cases, a medical device manufacturer might create a fix or mitigation for a vulnerability that needs to be reviewed and approved by the FDA, although the FDA "does not typically need to review changes made to medical devices solely to strengthen cybersecurity." [1] This is a distinct, important phase that precludes availability of an official patch. The FIRST CVSS v3.0 specification does not support representing this phase, but the rubric could be extended to account for it.

=== Report Confidence (RC) ===

Type: Impact/Temporal

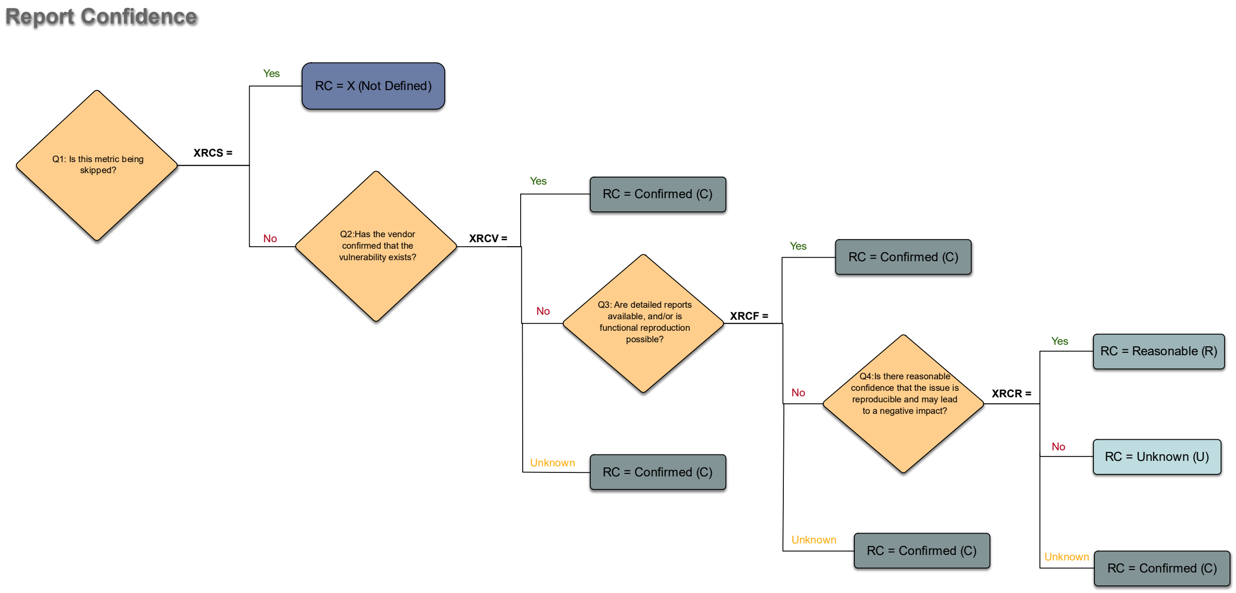
Specification: https://www.first.org/cvss/specification-document#3-3-Report-Confidence-RC

Q1 (XRCS). Is this metric being skipped?

- **No: Set RC="X".** Enter "NA" for remaining questions and move to the next metric.
- **Yes: Q2 (XRCV). Has the vendor confirmed that the vulnerability exists?**
  - **Yes: RC = "C" (Confirmed).**
  - **No: Q3 (XRCF): Are detailed reports available, and/or is functional reproduction possible?**
    - **Yes: RC = "C" (Confirmed).**
    - **No: Q4 (XRCR). Is there reasonable confidence that the issue is reproducible and may lead to a negative impact?**
      - **Yes: RC = "R" (Reasonable).**
      - **No: RC = "U" (Unknown).**
      - **Unknown: RC = "R" (Reasonable).**
    - **Unknown: RC = "C" (Confirmed).**
  - **Unknown: RC = "C" (Confirmed).**

[1] FDA Fact Sheet: "The FDA's Role in Medical Device Cybersecurity: Dispelling Myths and Understanding Facts". https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf

Report Confidence Decision Flow


Report Confidence
Q1: Is this metric being skipped?
XRCS =
Yes
RC = X (Not Defined)
No
Q2:Has the vendor confirmed that the vulnerability exists?
XRCV =
Yes
RC = Confirmed (C)
No
Q3: Are detailed reports available, and/or is functional reproduction possible?
Unknown
RC = Confirmed (C)
XRCF =
Yes
RC = Confirmed (C)
No
Q4:Is there reasonable confidence that the issue is reproducible and may lead to a negative impact?
Unknown
RC = Confirmed (C)
XRCR =
Yes
RC = Reasonable (R)
No
RC = Unknown (U)
Unknown
RC = Confirmed (C)

Report Confidence Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Report Confidence Skipped (XRCS)	Yes (Y) No (N)
Q2: Has the vendor confirmed that the vulnerability exists?	Extended Report Confidence Vendor Confirmed (XRCV)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Are detailed reports available, and/or is functional reproduction possible?	Extended Report Confidence Functional Reproduction (XRCF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is there reasonable confidence that the issue is reproducible and may lead to a negative impact?	Extended Report Confidence Reproducible (XRCR)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Working Group Discussion

In some cases, a vulnerability might be actively disputed between the researcher and the manufacturer. It is not clear whether (or how) unresolved disputes should be captured in the rubric. The FIRST CVSS v3.0 specification does not directly support the ability for the analyst to state that while a report has not been verified by the vendor, it is assumed to be correct because it was published by a trusted researcher or third-party coordinator. Perhaps the extended vector could be modified to capture this additional consideration.

=========== Environmental Metric Group ============

=== Confidentiality Requirement (CR) ===

Type: Impact/Environment

Specification: https://www.first.org/cvss/specification-document#4-1-Security-Requirements-CR-IR-AR

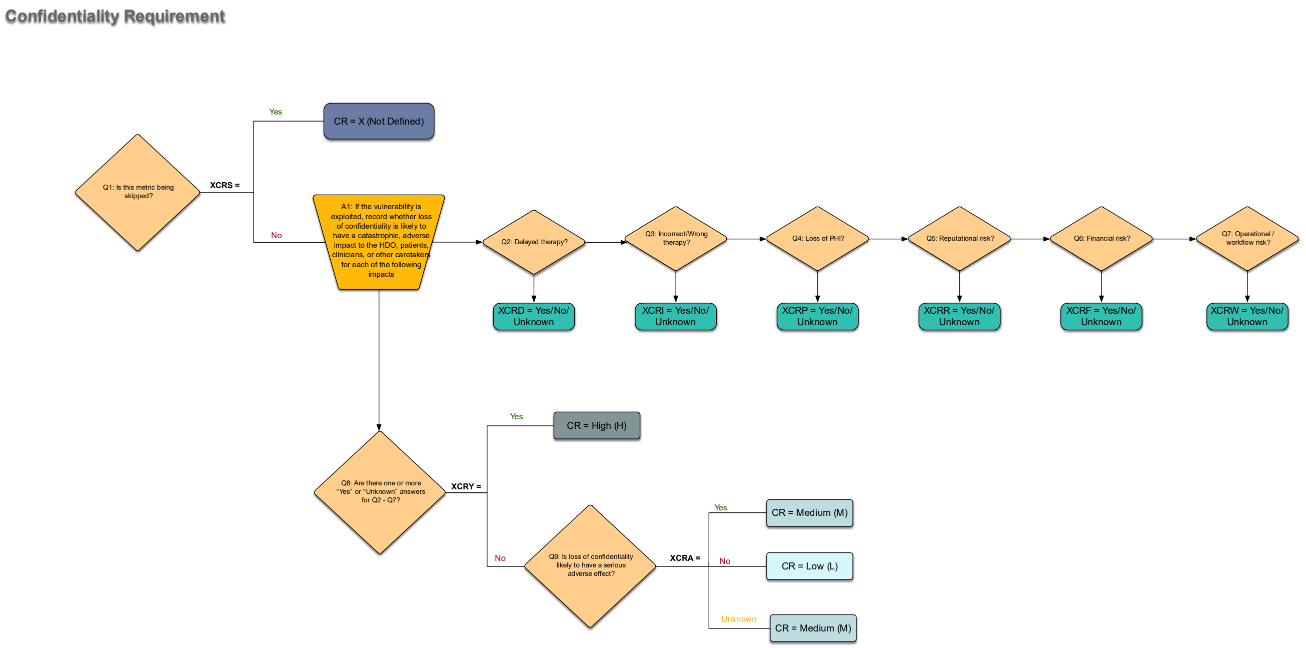
Q1 (XCRS). Is this metric being skipped?

- **Yes: set CR=”X” (Not Defined).** Enter “NA” for the remaining questions and move to the next metric.
- **No: Action 1. If the vulnerability is exploited, record whether loss of confidentiality is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts:**
  - **Q2. Delayed therapy? XCRD=Yes/No/Unknown.** Go to next question.
  - **Q3. Incorrect/Wrong therapy? XCRI=Yes/No/Unknown.** Go to next question.
  - **Q4: Loss of PHI? XCRP=Yes/No/Unknown.** Go to next question.
  - **Q5: Reputational risk? XCRR=Yes/No/Unknown.** Go to next question.
  - **Q6: Financial risk? XCRF=Yes/No/Unknown.** Go to next question.
  - **Q7: Operational/workflow risk? XCRW=Yes/No/Unknown.** Go to next question.

Q8 (XCRY). Are there 1 or more “Yes” or “Unknown” answers for Q2 through Q7?

- **Yes: CR = “H” (High)**
- **No: Q9 (XCRA). Is loss of confidentiality likely to have a serious adverse effect?**
  - **Yes: CR = “M” (Medium)**
  - **No: CR = “L” (Low).** Loss of confidentiality is likely to have limited or no adverse effect.
  - **Unknown: CR = “M” (Medium)**

Confidentiality Requirement Decision Flow


Confidentiality Requirement
Q1: Is this metric being skipped?
XCRS =
Yes
CR = X (Not Defined)
No
A1: If the vulnerability is exploited, record whether loss of confidentiality is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts
Q2: Delayed therapy?
XCRD = Yes/No/ Unknown
Q3: Incorrect/Wrong therapy?
XCRI = Yes/No/ Unknown
Q4: Loss of PHI?
XCRP = Yes/No/ Unknown
Q5: Reputational risk?
XCRR = Yes/No/ Unknown
Q6: Financial risk?
XCRF = Yes/No/ Unknown
Q7: Operational / workflow risk?
XCRW = Yes/No/ Unknown
Q8: Are there one or more "Yes" or "Unknown" answers for Q2 - Q7?
XCRY =
Yes
CR = High (H)
No
Q9: Is loss of confidentiality likely to have a serious adverse effect?
XCRA =
Yes
CR = Medium (M)
No
CR = Low (L)
Unknown
CR = Medium (M)

Confidentiality Requirement Extended Vector

Question	Element	Values
Q1. Is this metric being skipped?	Extended Confidentiality Requirement Skipped (XCRS)	Yes (Y) No (N)
Q2: Does loss of confidentiality have a catastrophic impact on delayed therapy?	Extended Confidentiality Requirement Delayed Therapy (XCRD)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Does loss of confidentiality have a catastrophic impact on incorrect/wrong therapy?	Extended Confidentiality Requirement Incorrect/Wrong Therapy (XCRI)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Does loss of confidentiality have a catastrophic impact on loss of PHI?	Extended Confidentiality Requirement PHI (XCRP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Does loss of confidentiality have a	Extended Confidentiality Requirement Reputational Risk (XCRR)	Yes (Y) No (N) Unknown (U)

catastrophic impact on reputational risk?		Not Answered (NA)
Q6: Does loss of confidentiality have a catastrophic impact on financial risk?	Extended Confidentiality Requirement Financial Risk (XCRF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q7: Does loss of confidentiality have a catastrophic impact on operational/workflow risk?	Extended Confidentiality Requirement Operational/Workflow Risk (XCRW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q8: Are there 1 or more "Yes" or "Unknown" answers for Q2 through Q7?	Extended Confidentiality Requirement Yes (XCRY)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q9: Is loss of confidentiality likely to have a serious adverse effect?	Extended Confidentiality Requirement Serious Adverse Effect (XCRA)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

The ability to read PHI could enable attackers to use the PHI to launch other attacks, e.g. by obtaining the patient's room, so it is currently regarded as catastrophic.

Working Group Discussion

The lack of consistency between the Confidentiality Impact values and the Confidentiality Requirement may cause confusion between readers. Currently the Confidentiality Requirement questions are a mix of technical effects (similar to the Confidentiality Impact questions) and higher-level organizational impacts. According to the CVSS specification, the CIA requirements are a way to assess the "importance of the affected IT asset to a user's organization, measured in terms of Confidentiality, Integrity, and Availability", so perhaps the Confidentiality Requirement questions should focus on higher-level impacts or harms. Are these the right questions to assess the importance of the affected device from a confidentiality perspective: patient safety, operations, compliance, reputation, financial?

=== Integrity Requirement (IR) ===

Type: Impact/Environment

Specification: https://www.first.org/cvss/specification-document#4-1-Security-Requirements-CR-IR-AR

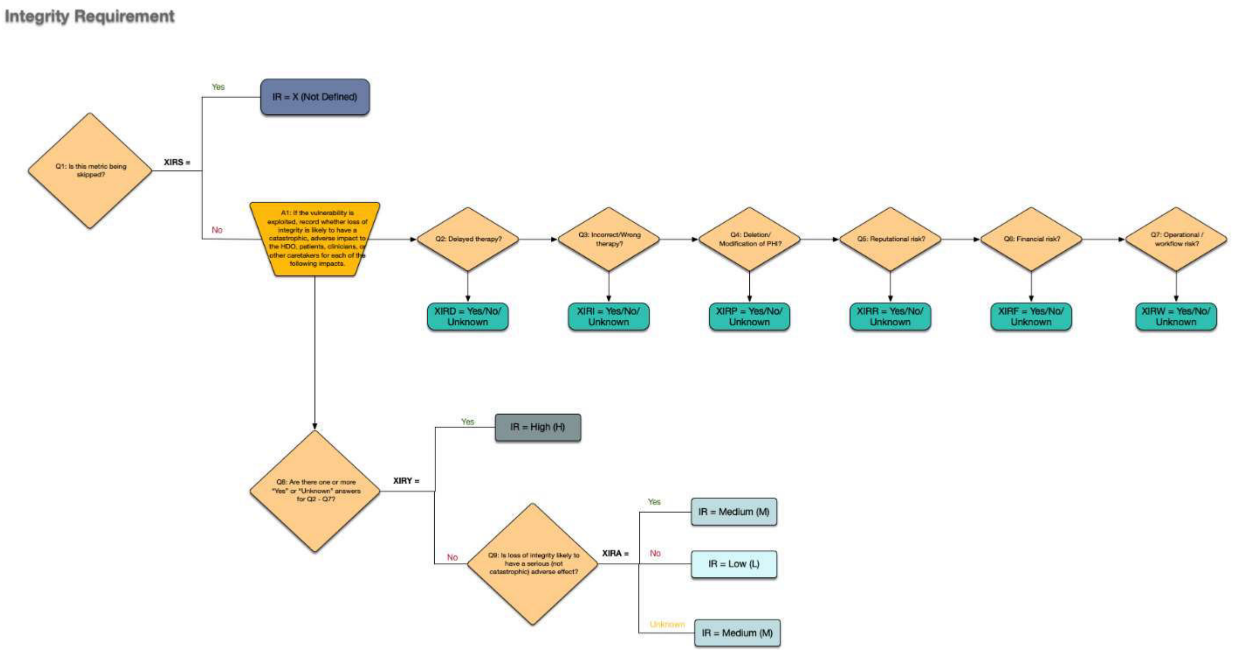
Q1 (XIRS). Is this metric being skipped?

- **Yes: set IR=”X” (Not Defined).** Enter “NA” for the remaining questions and move to the next metric.
- **No: Action 1. If the vulnerability is exploited, record whether loss of integrity is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts:**
  - **Q2. Delayed therapy? XIRD=Yes/No/Unknown.** Go to next question.
  - **Q3. Incorrect/Wrong therapy? XIRI=Yes/No/Unknown.** Go to next question.
  - **Q4: Deletion or modification of PHI? XIRP=Yes/No/Unknown.** Go to next question.
  - **Q5: Reputational risk? XIRR=Yes/No/Unknown.** Go to next question.
  - **Q6: Financial risk? XIRF=Yes/No/Unknown.** Go to next question.
  - **Q7: Operational / workflow risk? XIRW=Yes/No/Unknown.** Go to next question

Q8 (XIRY). Are there 1 or more “Yes” or “Unknown” answers for Q2 through Q7?

- **Yes: IR = “H” (High)**
- **No: Q9 (XIRA). Is loss of integrity likely to have a serious (not catastrophic) adverse effect?**
  - **Yes: IR = “M” (Medium)**
  - **No: IR = “L” (Low).** Loss of integrity is likely to have limited or no adverse effect.
  - **Unknown: IR = “M” (Medium)**

Integrity Requirement Decision Flow


Integrity Requirement
Q1: Is this metric being skipped?
XIRS =
Yes
IR = X (Not Defined)
No
A1: If the vulnerability is exploited, record whether loss of integrity is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts.
Q2: Delayed therapy?
XIRD = Yes/No/Unknown
Q3: Incorrect/Wrong therapy?
XIRI = Yes/No/Unknown
Q4: Deletion/Modification of PHI?
XIRP = Yes/No/Unknown
Q5: Reputational risk?
XIRR = Yes/No/Unknown
Q6: Financial risk?
XIRF = Yes/No/Unknown
Q7: Operational / workflow risk?
XIRW = Yes/No/Unknown
Q8: Are there one or more "Yes" or "Unknown" answers for Q2 - Q7?
XIRY =
Yes
IR = High (H)
No
Q9: Is loss of integrity likely to have a serious (not catastrophic) adverse effect?
XIRA =
Yes
IR = Medium (M)
No
IR = Low (L)
Unknown
IR = Medium (M)

Integrity Requirement Extended Vector

Question	Element	Values
Q1. Is this metric being skipped?	Extended Integrity Requirement Skipped (XIRS)	Yes (Y) No (N)
Q2: Does loss of integrity have a catastrophic impact on delayed therapy?	Extended Integrity Requirement Delayed Therapy (XIRD)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Does loss of integrity have a catastrophic impact on incorrect/wrong therapy?	Extended Integrity Requirement Incorrect/Wrong Therapy (XIRI)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Does loss of integrity have a catastrophic impact on deletion or modification of PHI?	Extended Integrity Requirement PHI (XIRP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Does loss of integrity have a catastrophic impact on reputational risk?	Extended Integrity Requirement Reputational Risk (XIRR)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q6: Does loss of integrity have a catastrophic impact on financial risk?	Extended Integrity Requirement Financial Risk (XIRF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q7: Does loss of integrity have a catastrophic impact on operational/workflow risk?	Extended Integrity Requirement Operational/Workflow Risk (XIRW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q8: Are there 1 or more "Yes" or "Unknown" answers for Q2 through Q7?	Extended Integrity Requirement Yes (XIRY)	Yes (Y) No (N) Not Answered (NA)
Q9: Is loss of integrity likely to have a serious adverse effect?	Extended Integrity Requirement Serious Adverse Effect (XIRA)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Modification of PHI could result in incorrect therapy, so it is regarded as catastrophic.

Working Group Discussion

From an HDO perspective, reputational or financial risk may be extremely important. The current rubric acknowledges this risk by dictating that the impact requirement is "High" if there is a catastrophic impact. For a safety-only rubric, financial and reputational impact would not be regarded as having a "High" requirement for integrity; perhaps "Medium" or even "Low" could be suggested in such cases.

The lack of consistency between the Integrity Impact values and the Integrity Requirement may cause confusion between readers. Currently the Integrity Requirement questions are a mix of technical effects (similar to the Integrity Impact questions) and higher-level organizational impacts. According to the CVSS specification, the CIA requirements are a way to assess the "importance of the affected IT asset to a user's organization, measured in terms of Confidentiality, Integrity, and Availability", so perhaps the Integrity Requirement questions should focus on higher-level impacts or harms. Are these the right questions to assess the importance of the affected device from an integrity perspective: patient safety, operations, compliance, reputation, financial?

=== Availability Requirement (AR) ===

Type: Impact/Environment

Specification: https://www.first.org/cvss/specification-document#4-1-Security-Requirements-CR-IR-AR

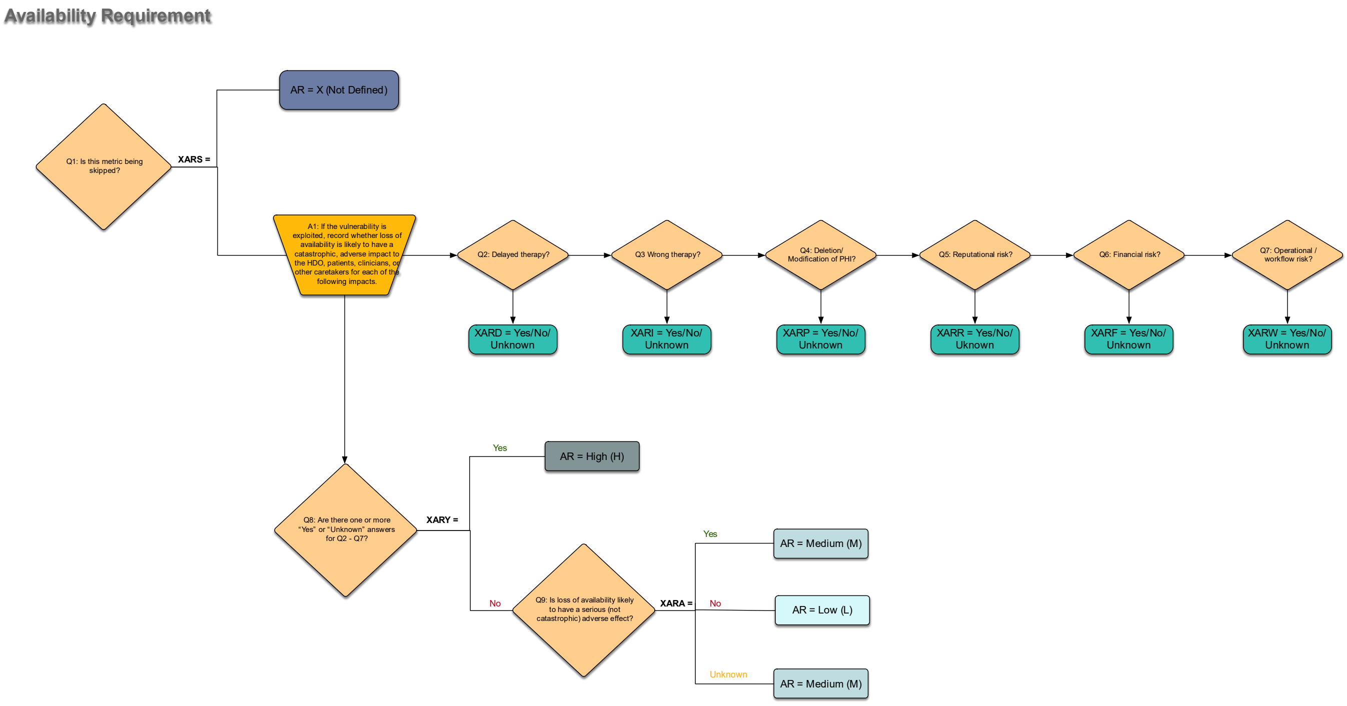
Q1 (XARS). Is this metric being skipped?

- **Yes: set AR="X" (Not Defined).** Enter "NA" for the remaining questions and move to the next metric.
- **No: Action 1. If the vulnerability is exploited, record whether loss of availability is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts:**
    - **Q2. Delayed therapy? XARD=Yes/No/Unknown.** Go to next question.
    - **Q3. Incorrect/Wrong therapy? XARI=Yes/No/Unknown.** Go to next question.
    - **Q4: Deletion or modification of PHI? XARP=Yes/No/Unknown.** Go to next question.
    - **Q5: Reputational risk? XARR=Yes/No/Unknown.** Go to next question.
    - **Q6: Financial risk? XARF=Yes/No/Unknown.** Go to next question.
    - **Q7: Operational/workflow risk? XARW=Yes/No/Unknown.** Go to next question.

Q8 (XARY). Are there 1 or more "Yes" or "Unknown" answers for Q2 through Q7?

- **Yes: AR = “H” (High)**
- **No: Q9 (XARA). Is loss of availability likely to have a serious (not catastrophic) adverse effect?**
    - **Yes: AR = “M” (Medium)**
    - **No: AR = “L” (Low).** Loss of availability is likely to have limited or no adverse effect.
    - **Unknown: AR = “M” (Medium)**

Availability Requirement Decision Flow


Availability Requirement
Q1: Is this metric being skipped?
XARS =
AR = X (Not Defined)
A1: If the vulnerability is exploited, record whether loss of availability is likely to have a catastrophic, adverse impact to the HDO, patients, clinicians, or other caretakers for each of the following impacts.
Q2: Delayed therapy?
XARD = Yes/No/ Unknown
Q3 Wrong therapy?
XARI = Yes/No/ Unknown
Q4: Deletion/ Modification of PHI?
XARP = Yes/No/ Unknown
Q5: Reputational risk?
XARR = Yes/No/ Uknown
Q6: Financial risk?
XARF = Yes/No/ Unknown
Q7: Operational / workflow risk?
XARW = Yes/No/ Unknown
Q8: Are there one or more “Yes” or “Unknown” answers for Q2 - Q7?
XARY =
Yes
AR = High (H)
No
Q9: Is loss of availability likely to have a serious (not catastrophic) adverse effect?
XARA =
Yes
AR = Medium (M)
No
AR = Low (L)
Unknown
AR = Medium (M)

Availability Requirement Extended Vector

Question	Element	Values
Q1. Is this metric being skipped?	Extended Availability Requirement Skipped (XARS)	Yes (Y) No (N)
Q2: Does loss of availability have a catastrophic impact on delayed therapy?	Extended Availability Requirement Delayed Therapy (XARD)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Does loss of availability have a catastrophic impact on incorrect/wrong therapy?	Extended Availability Requirement Incorrect/Wrong Therapy (XARI)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Does loss of availability have a catastrophic impact on deletion or modification of PHI?	Extended Availability Requirement PHI (XARP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Does loss of availability have a catastrophic impact on reputational risk?	Extended Availability Requirement Reputational Risk (XARR)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q6: Does loss of availability have a catastrophic impact on financial risk?	Extended Availability Requirement Financial Risk (XARF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q7: Does loss of availability have a catastrophic impact on operational/workflow risk?	Extended Availability Requirement Operational/Workflow Risk (XARW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q8: Are there 1 or more "Yes" or "Unknown" answers for Q2 through Q7?	Extended Availability Requirement Yes (XARY)	Yes (Y) No (N) Not Answered (NA)
Q9: Is loss of availability likely to have a serious adverse effect?	Extended Availability Requirement Serious Adverse Effect (XARA)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Working Group Discussion

Inability to read PHI could result in delayed or incorrect therapy, so it is regarded as catastrophic.

From an HDO perspective, reputational or financial risk may be extremely important. The current rubric acknowledges this risk by dictating that the impact requirement is "High" if there is a catastrophic impact. For a safety-only rubric, financial and reputational impact would not be regarded as having a “High” requirement for Availability; perhaps “Medium” or even “Low” could be suggested in such cases.

The lack of consistency between the Availability Impact values and the Availability Requirement may cause confusion between readers. Currently the Availability Requirement questions are a mix of technical effects (similar to the Availability Impact questions) and higher-level organizational impacts. According to the CVSS specification, the CIA requirements are a way to assess the “importance of the affected IT asset to a user's organization, measured in terms of Confidentiality, Integrity, and Availability”, so perhaps the Availability Requirement questions should focus on higher-level impacts or harms. Are these the right questions to assess the importance of the affected device from an availability perspective: patient safety, operations, compliance, reputation, financial?

=== Challenges with Modified Base Metrics ===

Working Group Discussion

CVSS v3.0 documentation contains little guidance for how to utilize modified base metrics, and there are no sample decision trees that could be adapted.

There are several challenges in defining a rubric for modified base metrics:

- The set of available values is exactly the same as the associated base metric. As a result, there is no ability to express mitigations in a way that affects the score. This is especially apparent in metrics such as Modified Attack Vector and Modified Attack Complexity; see the rubric for more details. These problems will be discussed with the FIRST CVSS SIG.
- Hospital/HDO environments vary widely, so their associated mitigations may vary widely.
- Some metrics might be very difficult or impossible for the HDO to modify, i.e., can only be implemented by the manufacturer.
- The HDO could make modifications that make exploitability or impact *worse* than in the original base score. This type of “upward trend” might not be well-tested in CVSS v3.0. It also makes this portion of the rubric more difficult to define, since one cannot necessarily default to the associated Base value. It might be ideal for each Modified item in the rubric to ask questions that reflect both “positive” and “negative” actions that might be undertaken by the HDO.

It is not clear whether each Modified Base Metric should contain the same decision tree as its associated Base Metric, or whether a customized decision tree should be created for each

Modified Base Metric. A customized tree might be too difficult to define and use, since Modified metrics will occur as the result of an application of various mitigations – which would introduce many more decision points – and the available mitigations are likely to be incomplete.

=== Modified Attack Vector (MAV) ===

Type: Exploitability/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

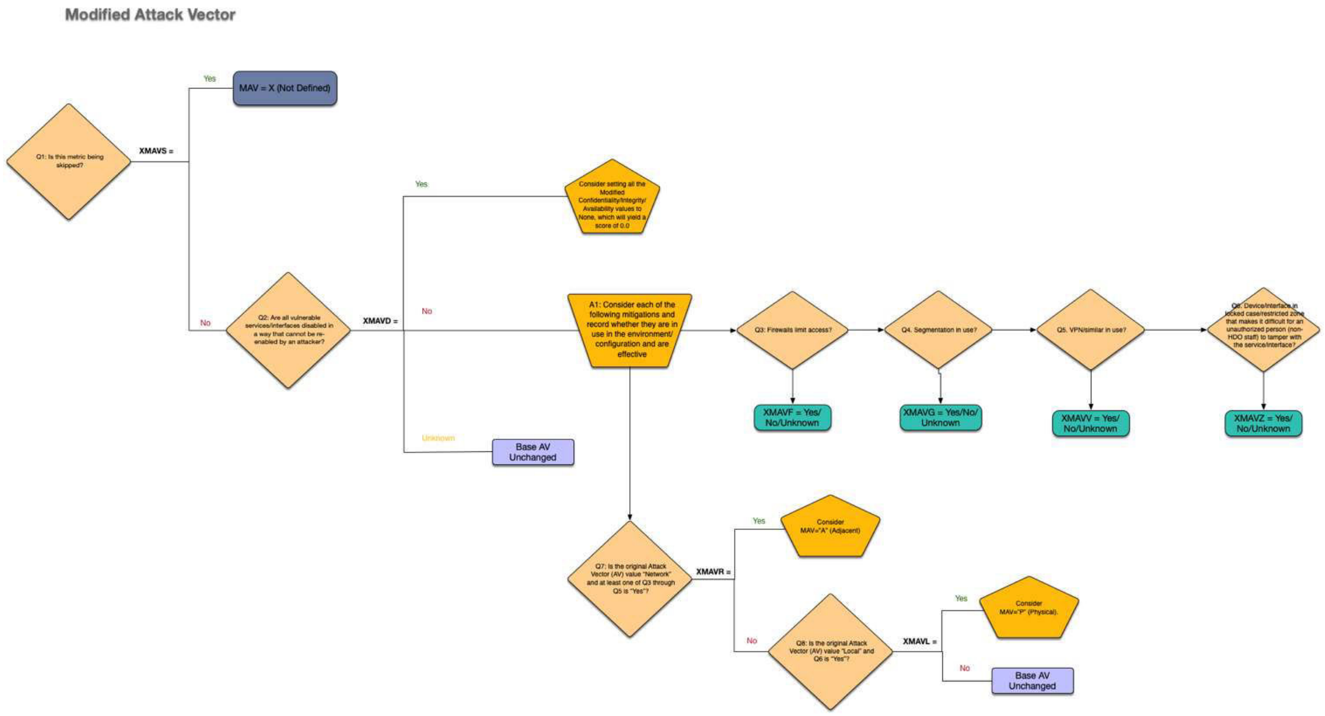
Q1 (XMAVS): Is this metric being skipped?

- **Yes: set MAV="X" (Not Defined).** Enter "NA" for the remaining questions and move to the next metric.
- **No: Q2 (XMAVD). Are all vulnerable services/interfaces disabled in a way that cannot be re-enabled by an attacker?**
    - **Yes:** Consider setting all the Modified Confidentiality/Integrity/Availability values to None, which will yield a score of 0.0.
    - **No: Action 1. Consider each of the following mitigations and record whether they are in use in the environment/configuration.** Answer each question Q3 through Q6. Only answer "Yes" if the mitigation applies to all vulnerable services/interfaces that are still enabled and if the mitigation is effective against the vulnerability.
        - **Q3. Firewalls limit access? XMAVF=Yes/No/Unknown.** Go to next question.
        - **Q4. Segmentation in use? XMAVG=Yes/No/Unknown.** Go to next question.
        - **Q5. VPN/similar in use? XMAVV=Yes/No/Unknown.** Go to next question.
        - **Q6. Device/interface in locked case/restricted zone that makes it difficult for an unauthorized person (non-HDO staff) to tamper with the service/interface without rapid detection by legitimate HDO staff? XMAVZ=Yes/No/Unknown.** Go to next question.
    - **Unknown: No change from the Base Attack Vector (AV).**

Q7 (XMAVR). Is the original Attack Vector (AV) value "Network" and at least one of Q3 through Q5 is "Yes"?

- **Yes: Consider MAV="A" (Adjacent).**
- **No: Q8 (XMAVL). Is the original Attack Vector (AV) value "Local" and Q6 is "Yes"?**
    - **Yes: Consider MAV="P" (Physical).**
    - **No: No change from the Base Attack Vector (AV).**

Modified Attack Vector Decision Flow


Modified Attack Vector
Q1: Is this metric being skipped?
XMAVS =
Yes
MAV = X (Not Defined)
No
Q2: Are all vulnerable services/interfaces disabled in a way that cannot be re-enabled by an attacker?
XMAVD =
Yes
Consider setting all the Modified Confidentiality/Integrity/ Availability values to None, which will yield a score of 0.0
No
A1: Consider each of the following mitigations and record whether they are in use in the environment/ configuration and are effective
Unknown
Base AV Unchanged
Q3: Firewalls limit access?
XMAVF = Yes/ No/Unknown
Q4. Segmentation in use?
XMAVG = Yes/No/ Unknown
Q5. VPN/similar in use?
XMAVV = Yes/ No/Unknown
Q6. Device/interface in locked case/restricted zone that makes it difficult for an unauthorized person (non-HDO staff) to tamper with the service/interface?
XMAVZ = Yes/ No/Unknown
Q7: Is the original Attack Vector (AV) value "Network" and at least one of Q3 through Q5 is "Yes"?
XMAVR =
Yes
Consider MAV="A" (Adjacent)
No
Q8: Is the original Attack Vector (AV) value "Local" and Q6 is "Yes"?
XMAVL =
Yes
Consider MAV="P" (Physical).
No
Base AV Unchanged

Modified Attack Vector Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Attack Vector Skipped (XMAVS)	Yes (Y) No (N)
Q2: Are all vulnerable services/interfaces disabled in a way that cannot be re-enabled by an attacker?	Extended Modified Attack Vector Services Disabled (XMAVD)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Firewalls limit access?	Extended Modified Attack Vector Firewall (XMAVF)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Q4: Segmentation in use?	Extended Modified Attack Vector Segmentation (XMAVG)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: VPN/similar in use?	Extended Modified Attack Vector VPN (XMAVV)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q6: Device/interface in locked case/restricted zone that makes it difficult for an unauthorized person (non-HDO staff) to tamper with the service/interface without rapid detection by legitimate HDO staff?	Extended Modified Attack Vector Restricted Zone (XMAVZ)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q7: Is the original Attack Vector (AV) value "Network" and at least one of Q3 through Q5 is "Yes"?	Extended Modified Attack Vector Remote Original (XMAVR)	Yes (Y) No (N) Not Answered (NA)
Q8: Is the original Attack Vector (AV) value "Local" and Q6 is "Yes"?	Extended Modified Attack Vector Local Original (XMAVL)	Yes (Y) No (N) Not Answered (NA)

Clarifications

Analysts should not consider protection mechanisms such as mutual authentication or device authentication, as these are more appropriate for Modified Attack Complexity (MAC) or Modified Privileges Required (MPR).

Unlike with the Confidentiality/Integrity/Availability Requirement metrics, the presence of "Unknown" answers is not considered in Q7, as it would lower the score.

Working Group Discussion

The rubric does not provide a clear, consistent answer if all affected services/interfaces are disabled. It could be argued that if the service is not running, then Confidentiality/Integrity/Availability impacts should be set to "None," which would effectively turn the CVSS score to 0.0. However, analysts might wish to capture the possibility in which an administrator violates policy and enables the service anyway, which could be represented using the attack vector required to perform administrator actions (such as Local or Physical). However, this could make the decision process too complex.

The recommendation for reducing “Remote” to “Adjacent” in Q7, and the “Local” to “Physical” recommendation in Q8, are likely inconsistent with how CVSS v3.0 defines it. However, mature HDOs that actively use security mechanisms such as firewalls or segmentation expect to be able to have the use of such mechanisms lower the environmental score, but strict compliance with CVSS v3.0 does not provide a way to lower the score. This difficulty will be raised with the FIRST CVSS SIG.

It is not clear whether – and how – to support analysis when multiple services or interfaces exist, and only some of them are disabled. In such cases, it might be appropriate to have the analyst independently assess each enabled service and ultimately select the “weakest” service to use to reflect the attack vector. However, such analysis might require more complex structures than the simple yes/no questions that the current rubric tries to use.

Examples

A device may be exposed to the Internet, accidentally or unintentionally, by a manufacturer’s service technician.

=== Modified Attack Complexity (MAC) ===

Type: Exploitability/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMACS): Is this metric being skipped?

- **Yes: set MAC=”X” (Not Defined).** Enter “NA” for remaining questions and move to the next metric.
    - **No: Action 1. Consider each of the following proposed mitigations and record whether they are in use in the environment/configuration.** Only answer “Yes” if the mitigation is in use and is effective against the vulnerability.
    - **Q2. Clinician badges using cryptography/NFC to authenticate to the device? XMACC=Yes/No/Unknown.**
    - **Q3. Biometric authentication (e.g., voice, fingerprints, eye)? XMACB=Yes/No/Unknown.**
    - **Q4. Multifactor authentication, tokens, etc.? XMACM=Yes/No/Unknown.** Go to Q5.

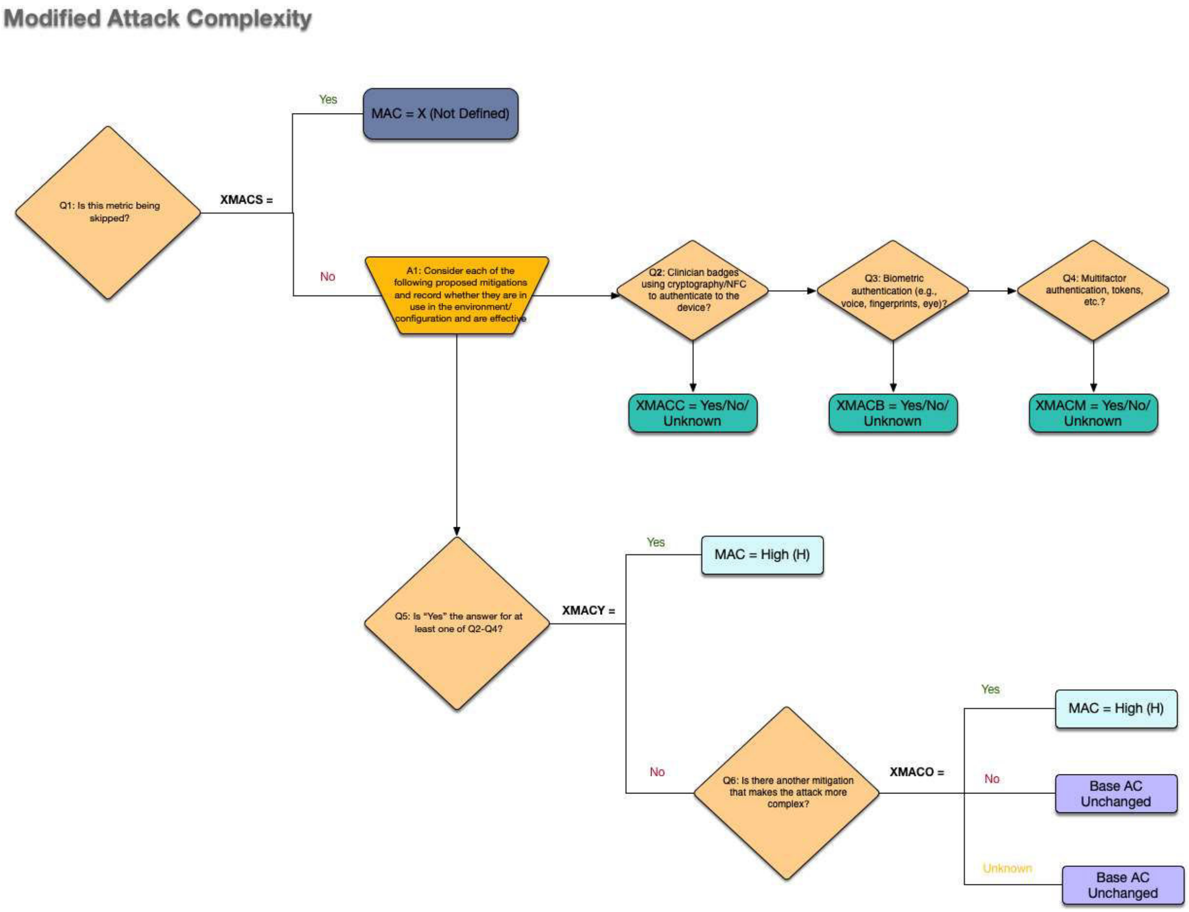
Q5 (XMACY): Is “Yes” the answer for at least one of Q2 through Q4?

- **Yes: MAC = “H” (High)**
- **No: Q6 (XMACO): Is there another mitigation that makes the attack more complex?** Note: the attacker is assumed to have complete knowledge of all inner workings of the product; therefore, complexity does NOT include difficulty of reverse-engineering code

or proprietary protocols, difficulty of writing exploit code, lack of access to equipment or manuals, etc.

- **Yes: MAC = "H" (High)**
- **No:** No change from base Attack Complexity (AC).
- **Unknown:** No change from base Attack Complexity (AC).

Modified Attack Complexity Decision Flow


Modified Attack Complexity
Q1: Is this metric being skipped?
XMACS =
Yes
MAC = X (Not Defined)
No
A1: Consider each of the following proposed mitigations and record whether they are in use in the environment/ configuration and are effective
Q2: Clinician badges using cryptography/NFC to authenticate to the device?
Q3: Biometric authentication (e.g., voice, fingerprints, eye)?
Q4: Multifactor authentication, tokens, etc.?
XMACC = Yes/No/ Unknown
XMACB = Yes/No/ Unknown
XMACM = Yes/No/ Unknown
Q5: Is "Yes" the answer for at least one of Q2-Q4?
XMACY =
Yes
MAC = High (H)
No
Q6: Is there another mitigation that makes the attack more complex?
XMACO =
Yes
MAC = High (H)
No
Base AC Unchanged
Unknown
Base AC Unchanged

Modified Attack Complexity Extended Vector

Question	Element	Values

Q1: Is this metric being skipped?	Extended Modified Attack Complexity Skipped (XMACS)	Yes (Y) No (N)
Q2: Clinician badges using cryptography/NFC to authenticate to the device?	Extended Modified Attack Complexity Clinician Badges (XMACC)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3. Biometric authentication (e.g., voice, fingerprints, eye)?	Extended Modified Attack Complexity Biometric Authentication (XMACB)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Multifactor authentication, tokens, etc.?	Extended Modified Attack Complexity Multifactor Authentication (XMACM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Is "Yes" the answer for at least one of Q2-Q4?	Extended Modified Attack Complexity Yes (XMACY)	Yes (Y) No (N) Not Answered (NA)
Q6: Is there another mitigation that makes the attack more complex?	Extended Modified Attack Complexity Other (XMACO)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations such as the following may be able to increase attack complexity:

- Increasing authentication requirements (e.g., device authentication with individual keys and PKI infrastructure, or one-time passwords)
- Changing manufacturer-default passwords or credentials, even if the same password is used across all devices within the HDO's environment.
- Enabling ASLR, Data Execution Protection, or other settings

Unlike with the Confidentiality/Integrity/Availability Requirement metrics, the presence of "Unknown" answers is not considered in Q5, as it would lower the score.

Working Group Discussion

There are probably many different changes that HDOs may implement that increase the attack complexity of existing vulnerabilities. These need to be identified and documented by the rubric as possible options.

=== Modified Privileges Required (MPR) ===

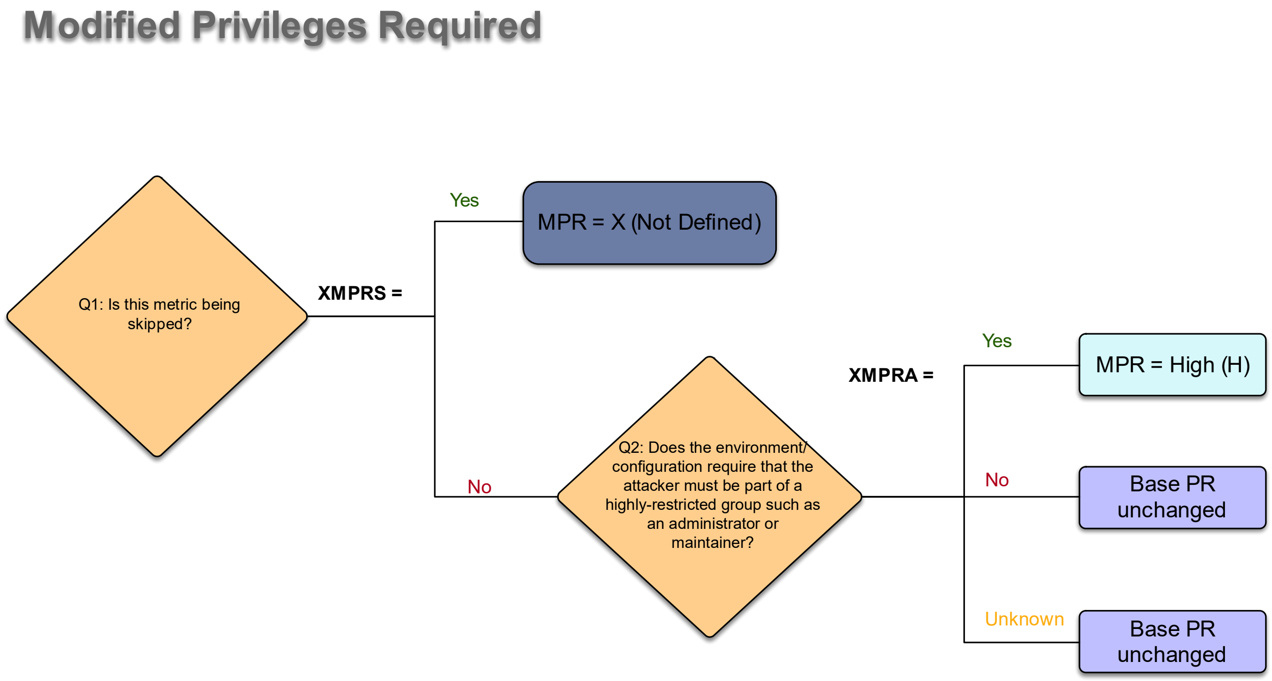
Type: Exploitability/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMPRS): Is this metric being skipped?

- **Yes: set MPR=”X” (Not Defined).** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XMPRA). Does the environment/configuration require that the attacker must be part of a highly-restricted group such as an administrator or maintainer?**
    - **Yes: MPR = “H” (High)**
    - **No:** No change from base Privileges Required (PR).
    - **Unknown:** No change from base Privileges Required (PR)

Modified Privileges Required Decision Flow


Modified Privileges Required
Q1: Is this metric being skipped?
XMPRS =
Yes
MPR = X (Not Defined)
No
Q2: Does the environment/ configuration require that the attacker must be part of a highly-restricted group such as an administrator or maintainer?
XMPRA =
Yes
MPR = High (H)
No
Base PR unchanged
Unknown
Base PR unchanged

Modified Privileges Required Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Privileges Required Skipped (XMPRS)	Yes (Y) No (N)
Q2: Does the environment/configuration require that the attacker must be part of a highly-restricted group such as an administrator or maintainer?	Extended Modified Privileges Required Administrator (XMPRA)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations such as the following may have an impact on Privileges Required (PR):

- Disabling services or interfaces that have weaker authentication or privileges
- Introduction of physical controls, such as:
  - Protective casing that requires a lock and key to open and access
  - Placement of device/ECP in restricted areas such as locked rooms
- Restrict functionality to a very limited group of users

=== Modified User Interaction (MUI) ===

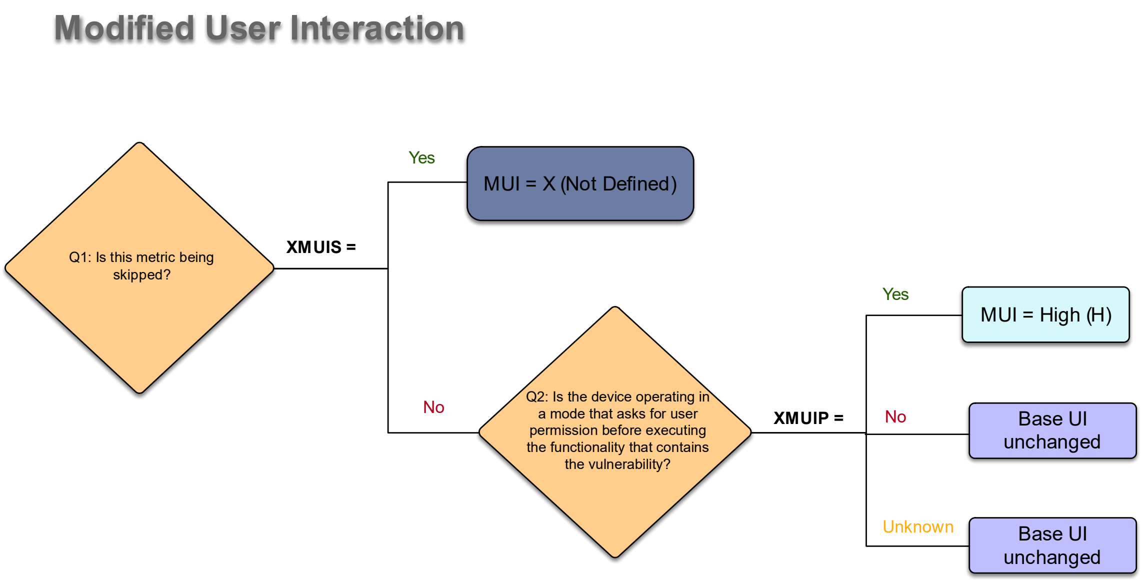
Type: Exploitability/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMUIS): Is this metric being skipped?

- **Yes: set MUI=”X” (Not Defined).** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XMUIP). Is the device operating in a mode that asks for user/admin permission before executing the functionality that contains the vulnerability?**
  - **Yes: MUI = “Y” (Yes)**
  - **No:** No change from base User Interaction (UI).
  - **Unknown:** No change from base User Interaction (UI).

Modified User Interaction Decision Flow


Modified User Interaction
Q1: Is this metric being skipped?
XMUIS =
Yes
MUI = X (Not Defined)
No
Q2: Is the device operating in a mode that asks for user permission before executing the functionality that contains the vulnerability?
XMUIP =
Yes
MUI = High (H)
No
Base UI unchanged
Unknown
Base UI unchanged

Modified User Interaction Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified User Interaction Skipped (XMUIS)	Yes (Y) No (N)
Q2: Is the device operating in a mode that asks for user permission before executing the functionality that contains the vulnerability?	Extended Modified User Interaction Permission Requested (XMUIP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations that might introduce a requirement for User Interaction (UI):

- Configuring the device to prompt the user to verify an action before executing the vulnerable functionality. (This might not be feasible with many devices/features.)
- Disabling automated actions that trigger the vulnerable functionality

Mitigations or actions that might reduce the User Interaction requirement:

- Disabling device prompts
- Creating programs/scripts that automatically ignore or accept warnings

Working Group Discussion

It is not clear whether there are realistic scenarios for which the HDO/admin has an ability to introduce user interaction when the Base group states that there is none; perhaps some devices or device classes have options to prompt users to accept otherwise-automatic interactions. On the other hand, the HDO can make some changes that reduce user interaction, e.g. by disabling prompts or implementing programs that automatically ignore/accept warnings.

=== Modified Scope (MS) ===

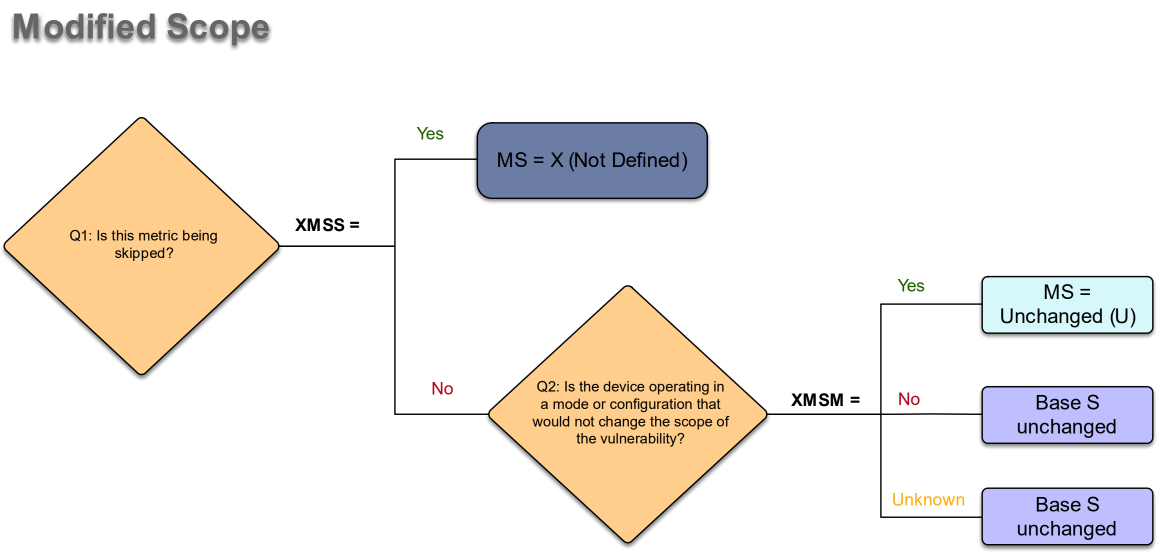
Type: Impact/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMSS): Is this metric being skipped?

- **Yes: set MS=”X” (Not Defined).** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XMSM). Is the device operating in a mode or configuration that would prevent the vulnerability’s scope from changing?**
  - **Yes: MS = “U” (Unchanged)**
  - **No:** No change from Base Scope (S).
  - **Unknown:** No change from base Scope (S).

Modified Scope Decision Flow


Modified Scope
Q1: Is this metric being skipped?
XMSS =
Yes
MS = X (Not Defined)
No
Q2: Is the device operating in a mode or configuration that would not change the scope of the vulnerability?
XMSM =
Yes
MS = Unchanged (U)
No
Base S unchanged
Unknown
Base S unchanged

Modified Scope Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Scope Skipped (XMSS)	Yes (Y) No (N)
Q2: Is the device operating in a mode or configuration that would prevent the vulnerability's scope from changing?	Extended Modified Scope Mode (XMSM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Working Group Discussion

It is not clear whether there are realistic scenarios for which the HDO/admin has an ability to prevent a device's scope from changing, if the scope can even be changed. It may be that a scope change is related directly to the device's intended functionality. Depending on the device class, workflow changes could introduce a manual sanity check that a clinician must approve before it is allowed to interact with "downstream" components. Additional investigation is needed.

=== Modified Confidentiality (MC) ===

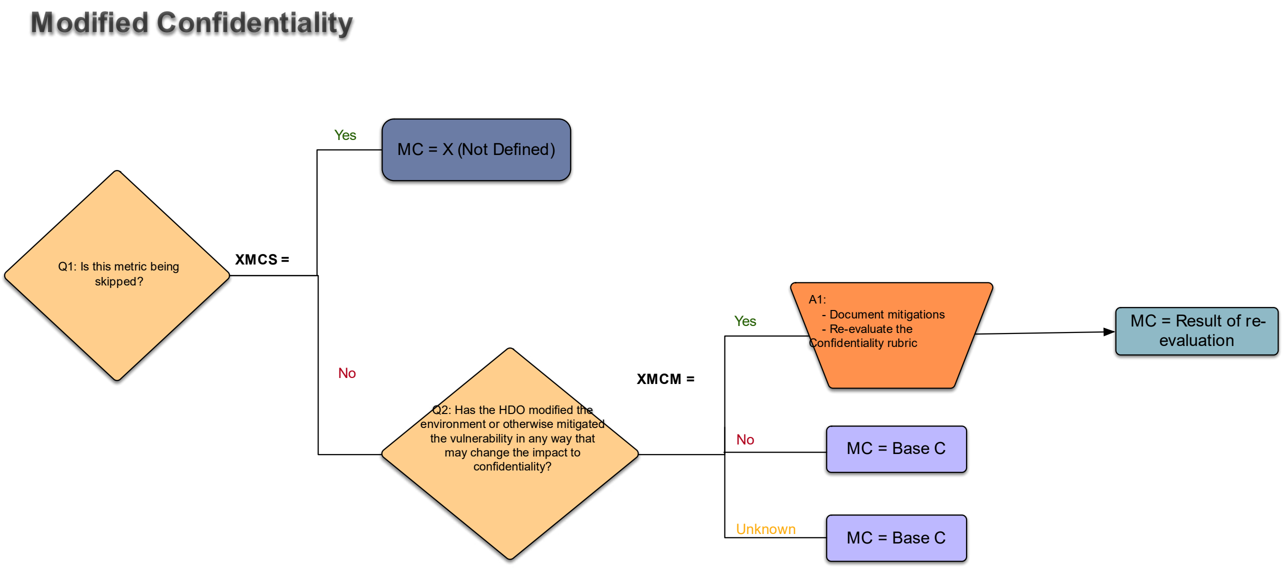
Type: Impact/Environment

Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMCS): Is this metric being skipped?

- **Yes: set MC="X" (Not Defined).** Enter "NA" for remaining questions and move to the next metric.
- **No: Q2 (XMCM): Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to confidentiality?**
  - **Yes: Action 1:** document the mitigations used; re-evaluate the rubric for Confidentiality; and determine the Modified Confidentiality (MC) score.
  - **No:** Use the Confidentiality value from the Base score.
  - **Unknown:** Use the Confidentiality value from the Base score.

Modified Confidentiality Decision Flow


Modified Confidentiality
Q1: Is this metric being skipped?
XMCS =
Yes
MC = X (Not Defined)
No
Q2: Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to confidentiality?
XMCM =
Yes
A1:
- Document mitigations
- Re-evaluate the Confidentiality rubric
MC = Result of re-evaluation
No
MC = Base C
Unknown
MC = Base C

Modified Confidentiality Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Confidentiality Skipped (XMCS)	Yes (Y) No (N)
Q2. Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to confidentiality?	Extended Modified Confidentiality Mitigation (XMCM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations that might improve confidentiality:

- Encrypted communications during transfer
- Encryption at rest before manual/semi-automated processes are activated, such as disk encryption
- Using the strongest encryption as built-in by the manufacturer
- Using external “dongles” or other mechanisms that provide end-to-end encryption at lower layers
- Reducing privileges to limit the amount of information that can be read (see Privileges Required)

Mitigations or other actions that might make confidentiality worse:

- Changing permissions for critical resources so that “Everyone” can read them. Such changes are often done for convenience or to ensure correct functioning with other software or capabilities on the device.
- Adding or increasing the privileges of unprivileged users, or changing the operations so that a “normal” user or guest is given admin-level privileges.

Working Group Discussion

It is not clear what options exist for the HDO/admin to reduce the confidentiality impact of a vulnerability. The manufacturer might provide certain encryption options of varying strengths, whether in transmission, at rest, or both. Alternately, the HDO might use VPN technology to create an encrypted layer of communications. The rubric could identify some of the most common mechanisms that improve the preservation of confidentiality; however, for each mechanism, there will need to be careful consideration for how to translate the mechanism's effectiveness into a Modified Confidentiality value.

=== Modified Integrity (MI) ===

Type: Impact/Environment

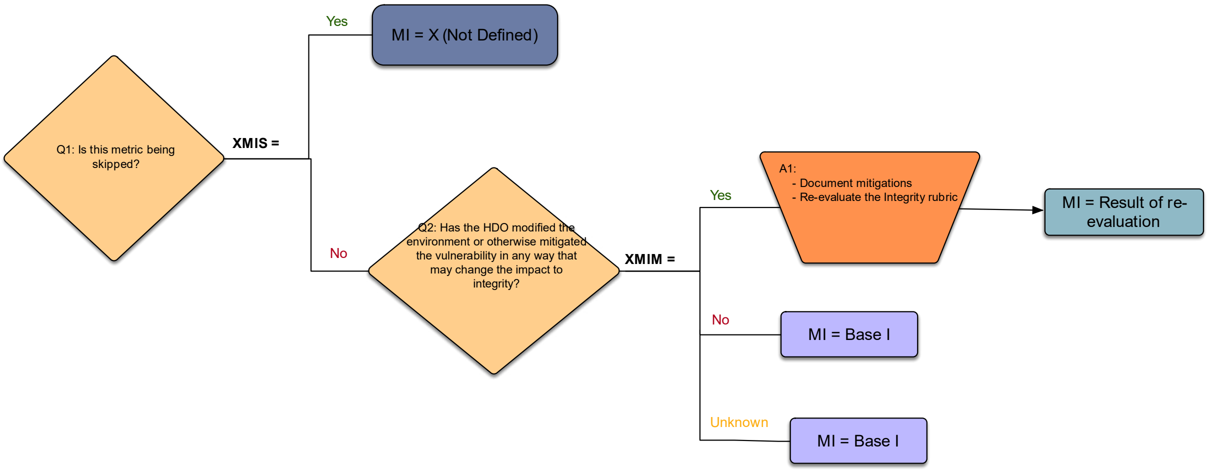
Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMIS): Is this metric being skipped?

- **Yes: set MI="X" (Not Defined).** Enter "NA" for remaining questions and move to the next metric.
- **No: Q2 (XMIM): Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to integrity?**
  - **Yes: Action 1:** document the mitigations used; re-evaluate the rubric for Integrity; and determine the Modified Integrity (MI) score.
  - **No:** Use the Integrity value from the Base score.
  - **Unknown:** Use the Integrity value from the Base score.

Modified Integrity Decision Flow

Modified Integrity


Q1: Is this metric being skipped?
XMIS =
Yes
MI = X (Not Defined)
No
Q2: Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to integrity?
XMIM =
Yes
A1:
- Document mitigations
- Re-evaluate the Integrity rubric
MI = Result of re-evaluation
No
MI = Base I
Unknown
MI = Base I

Modified Integrity Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Integrity Skipped (XMIS)	Yes (Y) No (N)
Q2: Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to integrity?	Extended Modified Integrity Mitigation (XMIM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations that might improve integrity:

- Reducing privileges to limit which data can be modified (see Privileges Required)
- Modification of permissions for critical resources, e.g. data files
- Selection of stronger integrity-check mechanisms (e.g. stronger hashing algorithms)
- Whitelisting of data
- Cryptographic signing data or applications

Mitigations or other actions that might make integrity worse:

- Setting permissions for critical resources so that “Everyone” can write to them. Such changes are often done for convenience or to ensure correct functioning with other software or capabilities on the device

Working Group Discussion

It is not clear what real-world options exist for the HDO/admin to reduce the integrity impact of a vulnerability. This may vary depending on the type of device and the granularity of control that the HDO/admin has on the operation of the device itself. Further discussion is necessary with HDO representatives and manufacturers who have offered configurable protection mechanisms that can be used to protect integrity.

=== Modified Availability (MA) ===

Type: Impact/Environment

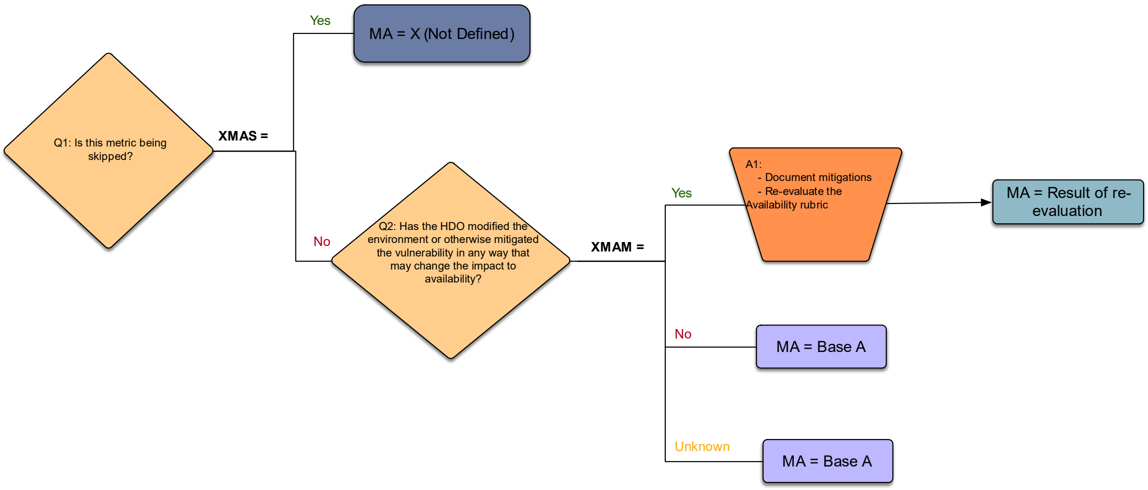
Specification: https://www.first.org/cvss/specification-document#4-2-Modified-Base-Metrics

Q1 (XMAS): Is this metric being skipped?

- **Yes: set MA=”X” (Not Defined).** Enter “NA” for remaining questions and move to the next metric.
- **No: Q2 (XMAM): Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to availability?**
    - **Yes: Action 1:** document the mitigations used; re-evaluate the rubric for Availability; and determine the Modified Availability (MA) score.
    - **No:** Use the Availability value from the Base score.
    - **Unknown:** Use the Availability value from the Base score.

Modified Availability Decision Flow

Modified Availability


Q1: Is this metric being skipped?
XMAS =
Yes
MA = X (Not Defined)
No
Q2: Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to availability?
XMAM =
Yes
A1:
- Document mitigations
- Re-evaluate the Availability rubric
MA = Result of re-evaluation
No
MA = Base A
Unknown
MA = Base A

Modified Availability Extended Vector

Question	Element	Values
Q1: Is this metric being skipped?	Extended Modified Availability Skipped (XMAS)	Yes (Y) No (N)
Q2: Has the HDO modified the environment or otherwise mitigated the vulnerability in any way that may change the impact to availability?	Extended Modified Availability Mitigation (XMAM)	Yes (Y) No (N) Unknown (U) Not Answered (NA)

Clarifications

Mitigations that might improve availability:

- Manual processes for replacement / hot-swap of backup devices
- Application-layer firewall that excludes availability-affecting interactions
- Process limits

- Throttling limits, e.g. reducing number of connections at the same time

Mitigations that might make availability worse:

- Use of excessively low throttling limits can make it easier for an attacker to trigger a denial of service.

Working Group Discussion

It is not clear what real-world options exist for the HDO/admin to reduce the availability impact of a vulnerability. This may vary depending on the type of device and the granularity of control that the HDO/admin has on the operation of the device itself. Further discussion is necessary with HDO representatives and manufacturers who have offered configurable protection mechanisms that can be used to protect availability.

=========== Other Metrics: CVSS v3.0 Gaps ============

Working Group Discussion

Several metrics have been identified that do not have direct correlations with CVSS v3.0, but they are important to some set of stakeholders in medical device security. These should be considered for integration into the rubric, even if they do not directly affect a CVSS-derived score.

- **Collateral Damage Potential (CDP)**– this was in CVSS v2 but removed in v3.0. Several working group members found this metric to be useful, since it explicitly considered "loss of life, physical assets, productivity or revenue." The current rubric represents many components of CDP as individual questions in the Confidentiality/Integrity/Availability metrics, but not all. For example, physical property damage (as included in CDP) is only indirectly referenced in the rubric in terms of financial or patient-safety impact. This may need closer consideration.
- **Target Distribution (TD)** - this was in CVSS v2 but removed in v3.0. This roughly captures the proportion of vulnerable systems. It appears to be an important consideration to the manufacturer, HDOs, FDA, and other stakeholders, but for various reasons. Independent of the *number* of devices or systems affected, the underlying "risk" for an individual device does not necessarily vary. It may be reasonable to have the rubric ask about target distribution, but to avoid having the answers contribute directly to the individual CVSS score.
- **Number of Affected Patients.** It may be important to capture the number of patients affected when considering prioritization of vulnerabilities, e.g. "one patient per device," "multiple patients per device," "all patients in a single hospital," and "all patients across all hospitals." For example, a vulnerability in an implanted pacemaker only affects one patient per implant, whereas a vulnerability in a programmer for the pacemaker might affect many patients, if it can be used to maliciously modify pacemaker settings of any patient that uses the pacemaker. There is no direct consideration of this within CVSS v3.0.

Systems-level risk assessment. Many devices are part of an integrated system, with an architecture involving many different components that all communicate independently.

- For example, a device that is physically attached to a patient might interact with a programmer or monitor, which also shares data across different servers within a cloud architecture. Risk assessment needs to consider the impacts and trust boundaries that individual components have on each other. While CVSS v3.0 has recognized “chains” of attacks, it is not necessarily ideal for guiding risk assessment of systems with multiple, independently-operating components. It is not clear how – or whether – to have this rubric be more precise in forcing (or guiding) the analyst to conduct the assessment from a more holistic perspective, instead of just evaluating the affected device/component in isolation.

=========== Rubric Answer Form (Scorecard) ============

The analyst could use the following answer form to record individual answers for the rubric.

The Notes section could be used to record the rationale for the answer, and/or to note when the analyst team disagrees or is uncertain about the best answer for the question.

Base Metric Group			
Field	**Question**	**Answer Code**	**Notes**
Attack Vector (AV)	Final Result		
	Q1 (XAVN)		
	Q2 (XAVT)		
	Q3 (XAVW)		
	Q4 (XAVR)		
	Q5 (XAVP)		
	Q5.1 (XAVPA)		
Attack Complexity (AC)	Final Result		
	Q1 (XACL)		
Privileges Required (PR)	Final Result		
	Q1 (XPRL)		
	Q2 (XPRZ)		
	Q3 (XPRS)		
User Interaction (UI)	Final Result		
	Q1 (XUI)		

Scope (S)	Final Result		
	Q1 (XS)		

<table>
<tr><th colspan="6">Confidentiality, Integrity, and Availability Impacts</th></tr>
<tr><th>Question: Read</th><th>Answer Code</th><th>Question: Modify</th><th>Answer Code</th><th>Question: Prevent Access</th><th>Answer Code</th></tr>
<tr><td>Q1.C (XCP)</td><td></td><td>Q1.I (XIP)</td><td></td><td>Q1.A (XAP)</td><td></td></tr>
<tr><td>Q1.1.C (XCPM)</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Q2.C (XCD)</td><td></td><td>Q2.I (XID)</td><td></td><td>Q2.A (XAD)</td><td></td></tr>
<tr><td>Q3.C (XCT)</td><td></td><td>Q3.I (XIT)</td><td></td><td>Q3.A (XAT)</td><td></td></tr>
<tr><td>Q4.C (XCW)</td><td></td><td>Q4.I (XIW)</td><td></td><td>Q4.A (XAW)</td><td></td></tr>
<tr><td>Q5.C (XCS)</td><td></td><td>Q5.I (XIS)</td><td></td><td>Q5.A (XAS)</td><td></td></tr>
<tr><td>Q6.C (XCO)</td><td></td><td>Q6.I (XIO)</td><td></td><td>Q6.A (XAO)</td><td></td></tr>
<tr><th colspan="2">Field</th><th>Question</th><th>Answer Code</th><th colspan="2">Notes</th></tr>
<tr><td colspan="2" rowspan="3">Confidentiality Impact (C)</td><td>Final Result</td><td></td><td colspan="2"></td></tr>
<tr><td>Q7 (XCH)</td><td></td><td colspan="2"></td></tr>
<tr><td>Q8 (XCL)</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="3">Integrity Impact (I)</td><td>Final Result</td><td></td><td colspan="2"></td></tr>
<tr><td>Q9 (XIH)</td><td></td><td colspan="2"></td></tr>
<tr><td>Q10 (XIL)</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="3">Availability Impact (A)</td><td>Final Result</td><td></td><td colspan="2"></td></tr>
<tr><td>Q11 (XAH)</td><td></td><td colspan="2"></td></tr>
<tr><td>Q12 (XAL)</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="6">Temporal Metric Group</th></tr>
</table>

Field	Question	Answer Code	Notes
Exploit Code Maturity (E)	Final Result		
	Q1 (XES)		
	Q2 (XEC)		
	Q2.1 (XEW)		
	Q3 (XEF)		
	Q4 (XEP)		
Remediation Level (RL)	Final Result		
	Q1 (XRLS)		
	Q2 (XRLO)		
	Q3 (XRLT)		
	Q4 (XRLW)		
Report Confidence (RC)	Final Result		
	Q1 (XRCS)		
	Q2 (XRCV)		
	Q3 (XRCF)		
	Q4 (XRCR)		
Environmental Metric Group			
Field	**Question**	**Answer Code**	**Notes**
Confidentiality Requirement (CR)	Final Result		
	Q1 (XCRS)		
	Q2 (XCRD)		
	Q3 (XCRI)		
	Q4 (XCRP)		
	Q5 (XCRR)		

	Q6 (XCRF)		
	Q7 (XCRW)		
	Q8 (XCRY)		
	Q9 (XCRA)		
Integrity Requirement (IR)	Final Result		
	Q1 (XIRS)		
	Q2 (XIRD)		
	Q3 (XIRI)		
	Q4 (XIRP)		
	Q5 (XIRR)		
	Q6 (XIRF)		
	Q7 (XIRW)		
	Q8 (XIRY)		
	Q9 (XIRA)		
Availability Requirement (AR)	Final Result		
	Q1 (XARS)		
	Q2 (XARD)		
	Q3 (XARI)		
	Q4 (XARP)		
	Q5 (XARR)		
	Q6 (XARF)		
	Q7 (XARW)		
	Q8 (XARY)		
	Q9 (XARA)		
Modified Attack Vector (MAV)	Final Result		
	Mitigations Applied		
	Q1 (XMAVS)		

	Q2 (XMAVD)		
	Q3 (XMAVF)		
	Q4 (XMAVG)		
	Q5 (XMAVV)		
	Q6 (XMAVZ)		
	Q7 (XMAVR)		
	Q8 (XMAVL)		
Modified Attack Complexity (MAC)	Final Result		
	Mitigations Applied		
	Q1 (XMACS)		
	Q2 (XMACC)		
	Q3 (XMACB)		
	Q4 (XMACM)		
	Q5 (XMACY)		
	Q6 (XMACO)		
Modified Privileges Required (MPR)	Final Result		
	Mitigations Applied		
	Q1 (XMPRS)		
	Q2 (XMPRA)		
Modified User Interaction (MUI)	Final Result		
	Mitigations Applied		
	Q1 (XMUIS)		
	Q2 (XMUIP)		
Modified Scope (S)	Final Result		
	Mitigations Applied		

	Q1 (XMSS)		
	Q2 (XMSM)		
Modified Confidentiality (MC)	Final Result		
	Mitigations Applied		
	Q1 (XMCS)		
	Q2 (XMCM)		
Modified Integrity (MI)	Final Result		
	Mitigations Applied		
	Q1 (XMIS)		
	Q2 (XMIM)		
Modified Availability (MA)	Final Result		
	Mitigations Applied		
	Q1 (XMAS)		
	Q2 (XMAM)		