Canon Medical Business Operations System Division Cybersecurity Vulnerability Handling

Version 2.0, 2026-04-01

■ DISCLOSURE POLICY

Canon Medical Business Operations System Division (hereinafter referred to as "our division") publishes cybersecurity vulnerabilities through security advisories when the following conditions are met.

- Cybersecurity vulnerability affects patient safety / essential performance and is or potentially an uncontrollable risk.
- Cybersecurity vulnerability which has been publicly released in the media.
- Cybersecurity vulnerability which has been disclosed from the security community.

■ RELATIONSHIP BETWEEN SECURITY RISK AND SAFTY RISK

Cybersecurity vulnerability may give impact to patient safety/essential performance. The risk management includes security risk and implements comprehensive management to reduce not only the risk associated with patient safety, but also includes the risk caused by cybersecurity.

When recognizing the security risk, there are cases where the impact on patient safety cannot be evaluated when malicious attacks that exploit security vulnerabilities cannot be predicted. For this reason, continuous monitoring of vulnerability information and malware information is critical.

■ TRIGGER OF CYBERSECURITY VULNERABILITY HANDLING

There are several types of triggers for cybersecurity vulnerability handling:

1. Vulnerability information for SOUP (Software Of Unknown Provenance) which is included in our products
2. Cybersecurity vulnerability reported from a third party

This document introduces the basic handling process for the above triggers.

1. CYBERSECURITY VULNERABILITY HANDLING PROCESS FOR SOUP IN PRODUCT

A cybersecurity vulnerability handling process typically consists of the following steps. The detailed handling process flow is described in Appendix 1.

A. Monitor cybersecurity information source and detect cybersecurity vulnerabilities

Our division's Product Security Incident Response Team (hereinafter referred to as "PSIRT") monitors cybersecurity vulnerability information about SOUP which is implemented on the medical devices and which may be attacked from outside actors.

The information sources are as follows.

· SOUP manufacturer's website

· ICS-CERT/JPCERT/JVN IPEDIA website

· Security tool manufacturer's website

The PSIRT collects the following information:

· CVE (Common Vulnerabilities and Exposures) ID

· Vulnerability Description

· CVSS (Common Vulnerability Scoring System) Base Metrics Score

B. Evaluate risk of cybersecurity vulnerabilities

If the CVSS base metrics score of the cybersecurity vulnerability is higher than the defined certain criteria, the PSIRT will evaluate the effect of the product along with the magnitude of the secondary damage which is based on the information of typical attack scenarios that exploit the vulnerability. A typical attack scenario is an active attack. In case of medical devices, other attack scenarios may be excluded since they are less likely. At that time, the cybersecurity vulnerabilities related SOUP components which are not permitted to be executed on the medical devices, are excluded. Such SOUP components include, although not limited to, web browsers, e-mail applications, and Office applications. With these considerations, the CVSS environment value is calculated. If the CVSS Environmental Metrics Score is more than the defined criteria, the PSIRT will identity the affected products.

C. Evaluate risk of patient hazard by cybersecurity vulnerabilities

Cybersecurity vulnerability does not necessarily lead directly to patient safety. Therefore, if threats such as "Tampering" or "Denial of Service" occur, the PSIRT will perform a comprehensive risk assessment of patient safety to analyzes the impact on patient safety. The risk assessment defines the severity along with the probability of patient harm. When the risk assessment result is greater than the defined criteria, the cybersecurity vulnerability is handled as a safety-related risk. In principle, multiple safety measures are implemented in the medical device so that the impact by malware, Ransomware, or other malicious attacks are mitigated.

D. Disclose cybersecurity vulnerabilities

If a remediation is required to mitigate the vulnerability, the PSIRT will release a security advisory which contains necessary information on the website.

The security advisory typically contains the following information:

· Description of the vulnerability with CVE ID and CVSS score

· Affected products
· Information on mitigating factors and workarounds

In case of a critical security risk with potential safety-impact, our division will promptly report to the applicable customers and corresponding agencies.

E. Investigate mitigation and plan to fix cybersecurity vulnerabilities

The PSIRT will update the security advisory as risk mitigation measures are provided during the active investigation. Risk mitigation measures are verified by the development group.

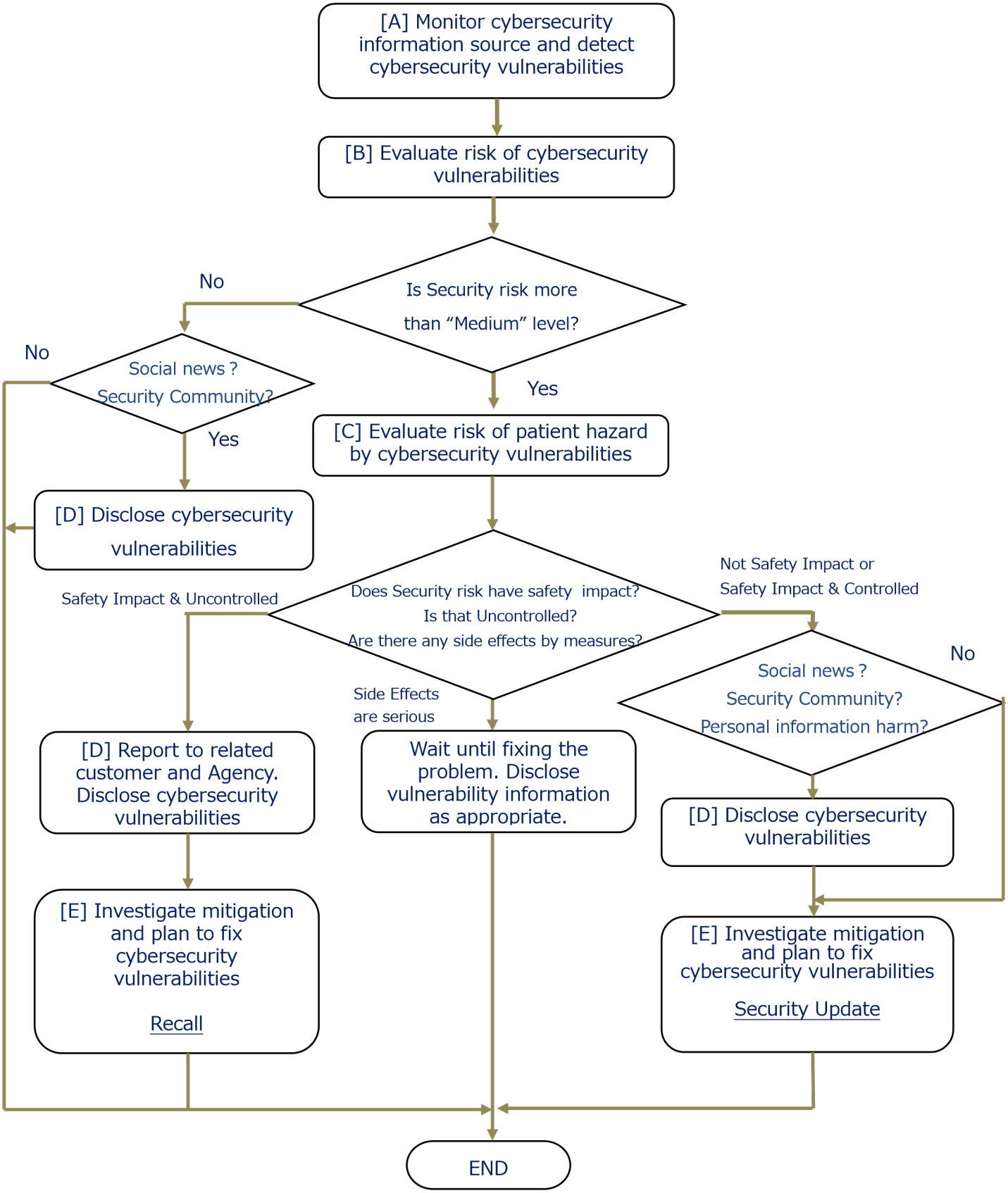
2. CYBERSECURITY VULNERABILITY HANDLING PROCESS FOR THIRD PARTY REPORT

The PSIRT welcomes cybersecurity vulnerability reports from researchers, industry groups, CERTs and any other sources. Please report the following information to our nearest branch office / distributor.

- Description of vulnerability, including proof-of-concept exploit code or network traces (if available)
- Potentially affected product, including model and firmware version (if available)
- Any public information or disclosure of the vulnerability
- Name of reporting actor
- Name of Healthcare facility or Integrated Delivery Network (IDN)
- Title
- Phone Number

With reported vulnerabilities, the PSIRT will internally investigate and will respond to the reporting actor in a timely fashion. The PSIRT may request further information from the reporting actor.

Appendix 1 CYBERSECURITY VULNERABILITY HANDLING PROCESS FLOW FOR SOUP IN PRODUCT



Revision Record V1.0 (2018-05-01): Publication

Revision Record V2.0 (2026-04-01): Company Name Change