

July 2026

Cybersecurity Vulnerability Management



Our approach

During the supported period of a respective product, Siemens Healthineers continuously monitors emerging vulnerabilities that become known and affect 3rd party components incorporated into that product to assess their impact on its security posture. This process takes into consideration the FDA¹ post-market guidance² and industry best practices and consists of the different phases depicted in Figure 1.



Figure 1: 3rd party component vulnerability assessment process at Siemens Healthineers

3rd party component threat intelligence

A central service at Siemens Healthineers monitors a variety of external sources for emerging vulnerabilities including US NIST³ NVD⁴ and the US CISA⁵ KEV⁶ catalog that are relevant for Siemens Healthineers' products based on a company-wide 3rd party component registry.

The Siemens Healthineers team analyzes and standardizes the 3rd party component vulnerability information and turns them into dedicated security notifications. Further sources of vulnerability information are periodically performed vulnerability scans by many product teams and input from security researchers according to our CVD⁷ process as described on our Cybersecurity homepage⁷.

Matching with product database

Siemens Healthineers maintains a product security inventory that contains the security information of Healthineers' products. This inventory includes SBOM⁸s

which list the 3rd party components utilized in a product. The inventory connects to the company-wide 3rd party component registry.

Security notifications are synchronized daily between both repositories using the available component identification information to filter for affected products.

Assessment by product experts

Product teams receive and process the security notifications applicable to their products⁹ through a workflow designed to facilitate consistency across the subsequent evaluation of vulnerabilities.

The responsible product experts assess the component level vulnerability information in the context of product design and intended use. Each vulnerability is assessed in accordance with the FDA post market guidance² for exploitability¹⁰. As a result of the assessment, a customer notice is created for most products, describing the vulnerability impact according to the categories depicted in Figure 2.

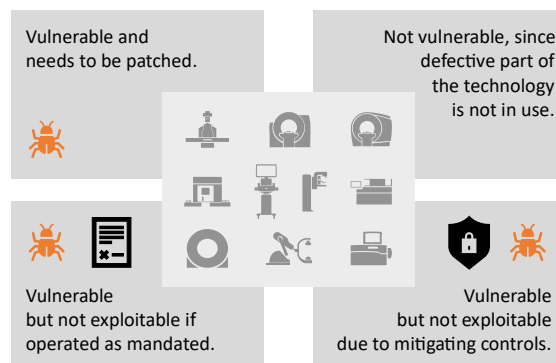


Figure 2: Evaluation result categories for assessed vulnerabilities

The evaluation results are approved by the responsible Cybersecurity Officer. Based on the assessed criticality and the product release, the evaluation results may be published to the customer portal¹¹.

In case of an exploitable vulnerability, the product teams also assess the severity and risk of patient harm. This allows Siemens Healthineers to take timely action on uncontrolled and controlled risks e.g. based on the FDA post market guidance².

Customer Communication and Patching

The Siemens Healthineers' vulnerability management process is designed to provide customers with¹¹:

- Prompt remediation of uncontrolled risks
- Transparency on the security status of their Siemens Healthineers' products
- Product specific threat assessments for relevant CVEs
- Information on how to mitigate potential risks

In the event of vulnerabilities posing an uncontrolled risk to patients¹³, information about the vulnerability will usually be made available within 30 days. In this case, patches (if available and validated) or other mitigations^{14,15} will usually be released within 60 days after the information becomes known to Siemens Healthineers.

Vulnerabilities posing a controlled risk for patients¹³, are handled by product teams in a best effort approach. Siemens Healthineers will decide at their discretion to disclose the related vulnerability assessments and/or to release patches or remediations^{14,15,16}. Patching cadence for controlled vulnerabilities varies across products based on product age, required validation effort, and experience with customer's uptake of patches.

Evaluation results and security patching information are made available to customers as Security Advisories or Vulnerability Assessments in the Siemens Healthineers fleet management portals teamplay Fleet¹¹ and/or MyVarian.com.

Update packages, where applicable, are made available through Smart Remote Services¹⁷ and/or teamplay Fleet⁷ respectively MyVarian.com for faster implementation by customers.

The onsite application of patches and other mitigations^{14,15} may be subject to additional charges, depending on the existing service agreement.

For all cloud solutions, Siemens Healthineers follows a pro-active risk mitigation technique by implementing continuous vulnerability management. We provide patching on a periodic basis, and/or as needed based on any critical events like zero-day vulnerabilities.

Siemens Healthineers actively participates in the Health-ISAC¹⁸ and will share information about critical and urgent vulnerabilities with them.

Component EOL¹⁹ handling strategy

Siemens Healthineers is monitoring 3rd party components for emerging EOL date information and will potentially plan replacing such components based on their potential impact on patient safety and overall product security in alignment with the product roadmap and its support level. The decision will be influenced by the likelihood of the said component being part of the attack surface, ie, whether an exploit path towards/including it exists.

1 Food and Drug Administration of the United States (FDA)

2 Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff (fda.gov)

3 United States National Institute of Standards and Technology (NIST)

4 National Vulnerability Database (NVD)

5 Cybersecurity and Infrastructure Security Agency (CISA)

6 Known Exploited Vulnerabilities Catalog (KEV)

7 Coordinated Vulnerability Disclosure (CVD): <https://www.siemens-healthineers.com/support-documentation/cybersecurity>

8 Software Bill of Materials (SBOM)

9 For products that have not reached end-of-support.

10 The classification of a vulnerability as exploitable or non-exploitable may be subject to customer's compliance with Siemens Healthineers' instructions for deployment and operation and application of any recommended security controls, if applicable.

11 For supported equipment. Requires a customer account in teamplay Fleet.

12 Common Vulnerabilities & Exposures (CVE)

13 As defined by the FDA post Market Guidance.

14 The implementation of patches and other mitigations may require customer action depending on the connectivity status of the system and the existing service agreement.

15 Other mitigations may include but are not limited to configuration or external changes on any of the layers of the technology stack of the product (i.e., application, operating system, communications or hardware).

16 In some cases, patches are provided as part of routine updates on a regular basis.

17 For supported and SRS connected equipment. SRS is subject to a separate contract and may not be available in all countries and/or for all modalities.

18 Information Sharing and Analysis Center (ISAC)

19 End of life (EOL)

Siemens Healthineers Headquarters

Siemens Healthineers AG
Siemensstrasse 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
[siemens-healthineers.com](https://www.siemens-healthineers.com)