

RFC 2350

Siemens Healthineers CSIRT

Published on 01.12.2023

Purpose

This document contains a description of the CSIRT of Siemens Healthineers in accordance with RFC 2350. It provides basic information about its channels of communication, and its roles and responsibilities.

Change History

Revision	Changes	Date
1.0	Initial Version	2023-12-01

Content

1	Document Information.....	3
1.1	Date of last update.....	3
1.2	Distribution list for notifications	3
1.3	Locations where this document may be found.....	3
1.4	Document identification	3
2	Contact Information.....	3
2.1	Name of the team	3
2.2	Address.....	3
2.3	Time zone	3
2.4	Telephone number	4
2.5	Facsimile number	4
2.6	Other telecommunications	4
2.7	Electronic mail address	4
2.8	Public keys and encryption information	4
2.9	Team members	4
2.10	Other information	4
3	Charter.....	4
3.1	Mission statement.....	4
3.2	Constituency.....	4
3.3	Sponsor and/or affiliation	4
3.4	Authority	5
4	Policies.....	5
4.1	Types of incidents and level of support	5
4.2	Co-operation, interaction, and disclosure of information	5
4.3	Communication and authentication	5
5	Services.....	5
5.1	Incident response.....	5
5.2	Incident technical analysis	6
5.3	Incident resolution/Mitigation	6
5.4	Incident reporting forms	6
5.5	Disclaimers	6

1 Document Information

1.1 Date of last update

Version 1.0, published on 2023/12/01.

1.2 Distribution list for notifications

There is no distribution list for notifications.

1.3 Locations where this document may be found

The current version of this document can be found at this URL.

1.4 Document identification

Title	RFC2350
Version	1.0
Document Date	2023-12-01
Expiration	This document is valid until superseded by a later version

2 Contact Information

2.1 Name of the team

Full Name	Siemens Healthineers CyberSecurity Incident Response Team
Short name	Siemens Healthineers CSIRT

2.2 Address

Siemens Healthineers CSIRT is a global team, and its members are distributed across the United States, Spain, Canada, Brazil, India, and Germany.

Address	Siemens Healthineers Henkestr. 127 91052 Erlangen Germany
----------------	--

2.3 Time zone

Siemens Healthineers CSIRT locations and time zones are Germany and Spain (UTC+01:00 and UTC+02:00 from April to October), Brazil (UTC-03:00) India (UTC+05:30) and Canada (UTC-08:00 and UTC-07:00 from March to November).

2.4 Telephone number

No public number is available.

2.5 Facsimile number

None.

2.6 Other telecommunications

None.

2.7 Electronic mail address

The preferred method to contact Siemens Healthineers CSIRT is to send an email to csirt@siemens-healthineers.com.

2.8 Public keys and encryption information

PGP is used for functional exchanges between Siemens Healthineers CSIRT and its peers, partners, and constituents.

Fingerprint	
	2F6F10718296C3D83CCCB39837F821AADDEA88B0

2.9 Team members

Siemens Healthineers CSIRT has 8 team members distributed across Spain, Germany, Canada, Brazil, and India.

2.10 Other information

General information about Cybersecurity at Siemens Healthineers can be found at this URL.

3 Charter

3.1 Mission statement

Siemens Healthineers CSIRT leads and coordinates the response to IT and OT cybersecurity Incidents within the company, ensuring their prompt resolution by conducting the necessary investigation activities and coordinating the implementation of containment measures.

3.2 Constituency

Siemens Healthineers CSIRT provides its services to all the internal users that manage or make use of IT/OT assets belonging to Siemens Healthineers as well as external third parties (e.g., external researchers, external communities) that want to report us potential cybersecurity incidents affecting our IT/OT infrastructure.

3.3 Sponsor and/or affiliation

Siemens Healthineers CSIRT is a global team that is part of the IT/OT Cybersecurity Operations team of Siemens Healthineers.

3.4 Authority

Siemens Healthineers CSIRT operates under the authority of the Corporate Cybersecurity Officer and is integral part of Siemens Healthineers IT.

Siemens Healthineers CSIRT is outlined within the parameters of the corporate Cybersecurity Management System (certified according to ISO 27001/27701) and operates in strict compliance with the terms and conditions defined by Siemens Healthineers, as well as the laws of the countries in which it operates.

4 Policies

4.1 Types of incidents and level of support

Siemens Healthineers CSIRT is authorized to handle any kind of IT/OT cybersecurity incident impacting Siemens Healthineers IT/OT assets and representing a threat to the confidentiality, integrity, and availability of our IT/OT assets, for instance:

- Successful attempts to gain unauthorized access to a system or its data.
- Disruption or denial of service with a malicious intent.
- Unauthorized use of a system for the processing or storage of data.
- Changes to a system's hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- Critical vulnerabilities that meet the criteria to require Special Vulnerability Handling.

The level of support depends on the incident severity and impact scale defined in the IT/OT Incident management internal instruction.

4.2 Co-operation, interaction, and disclosure of information

All information is held confidentially by Siemens Healthineers CSIRT, and information is tagged accordingly with TLP framework.

Siemens Healthineers CSIRT operates in accordance with the Cybersecurity Management System of Siemens Healthineers that is aligned with the local regulations of the countries where the company operates.

4.3 Communication and authentication

Siemens Healthineers CSIRT respects the sensitivity categorization assigned by the originators of the information that is shared by any of the available sources of communication.

For exchanging information that does not contain sensitive information, Siemens Healthineers CSIRT uses conventional methods such as unencrypted email.

For sensitive information, PGP is used (please, refer to section 2.8).

5 Services

5.1 Incident response

Siemens Healthineers CSIRT leads and coordinates the response to cybersecurity incidents affecting Siemens Healthineers IT/OT assets. The team performs the necessary technical investigations to determine the root cause of the incident, and it delivers effective containment strategies and drives the remediation activities.

5.2 Incident technical analysis

Siemens Healthineers CSIRT reviews the incidents that are reported on the different available channels and performs their triage, which includes their categorization, and prioritization based on their severity.

After their initial triage, additional information is requested, and forensic artifacts are collected in order to conduct the technical analysis of the compromised systems and identify the scope of the incidents as well as their root cause.

Siemens Healthineers CSIRT is also responsible for defining the response strategy and ensuring that the necessary containment activities are applied.

5.3 Incident resolution/Mitigation

Siemens Healthineers CSIRT is responsible for identifying the activities that are needed for a successful recovery and ensuring that they are performed, providing guidance, and involving the necessary entities.

Once the remediation is finalized, Siemens Healthineers CSIRT documents the closure of the incident and the lessons learned.

5.4 Incident reporting forms

Cybersecurity incidents should be reported to the Siemens Healthineers CSIRT by email at csirt@siemens-healthineers.com, preferably encrypted with our PGP public key (please, refer to section 2.8).

It would be necessary to include, at least, the following information:

Contact details	Name of the reporter, organization contact details (i.e., name, email address and telephone number).
Summary of the incident	Description of the potential incident including, if possible, the estimated impact.
Source of the cybersecurity incident/threat	Including, if possible, its IP address, hostname, location or application name.
How the cybersecurity incident/threat has been detected	Including details about the observations that led to the discovery of the incident. If any evidence is available, it should be attached.
Affected asset	Including, if possible, its IP address, hostname, location, or application name.

5.5 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Siemens Healthineers CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.