1. Document Information

This document contains a description of Bosch CERT according to IETF RFC2350. It provides basic information about the Bosch CERT, its communication channels, and its services, roles and responsibilities

1.1. Date of Last Update

Version 1.5, Sep 2025

1.2. Distribution List for Notifications

There is no distribution list for notifications as of 2025/07.

1.3. Locations where this Document May Be Found

The current version of Bosch CERT's RFC2350

- is available within our Bosch internal accessible Docupedia space (with some additional internal links)
- is published at https://psirt.bosch.com/

1.4. Authenticating this Document

This document has been digitally signed with the Bosch CERT's S/MIME-key. See section 2.8 for more details.

1.5. Document Identification

Title: "RFC 2350 Description of Bosch CERT"

Current Version: 1.5

Initial Date: 16.02.2016

Document classification: Internal

Expiration: This document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

Bosch Computer Emergency Response Team

Short name: Bosch CERT

2.2. Address

Robert Bosch GmbH
C/CYT-IR - Bosch CERT
Wernerstraße 51
70469 Stuttgart
GERMANY

2.3. Time Zone

Europe/Berlin (GMT+0100, and GMT+0200 on DST)

2.4. Telephone Number

Bosch CERT Hotline: +49(711)811-24611

2.5. Facsimile Number

n.a.

2.6. Other Telecommunication

n.a.

2.7. Electronic Mail Address

security@bosch.com

For secure, PGP-encrypted communication, please use the key associated with psirt@bosch.com as detailed in section 2.8.

2.8. Public Keys and Other Encryption Information

Bosch CERT uses S/MIME to digitally encrypt and sign emails exchanged with its constituency. This ensures data confidentiality, integrity and non-repudiation. The current valid S/MIME certificate can be found under: https://certsrv.bosch.com.

For PGP encrypted email please use psirt@bosch.com with the key material to found here: https://psirt.bosch.com/

2.9. Operating Hours

Standard Hours: 09:00 - 23:00 (GMT+0100, and GMT+0200 on DST) Monday to Friday (closed on Saturday, Sunday and public holidays Baden-Wuerttemberg, Germany)

After Hours: An on-call team is available for critical emergencies.

In addition, we can be contacted 24/7 via IT service desk.

2.10. Team Members

Head of Bosch CERT: **Stefan Lindner (C/CYC C/CYT)**

The list of the team members can be found on the corresponding internal BGN sub pages.

2.11. Other Information

General information about Bosch CERT as well as links to various security resources can be found in the internal Bosch network.

3. Charter

3.1. Mission Statement

"We combine offensive and defensive skills - before, during, and after cybersecurity threats emerge to enhance the resilience of Bosch."

Bosch CERT will operate according to the following key values:

- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues

- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of good practices between constituents and with peers
- Fostering a culture of openness within a protected environment, operating on a need to know basis

3.2. Constituency

The constituency of Bosch CERT is equivalent to the union of the scopes of the internal Corporate Directives *Information Security and Data Protection* and *Cybersecurity*.

3.3. Sponsorship and/or Affiliation

Bosch CERT is sponsored and mandated by the Corporate Department “Cybersecurity” and the Corporate Department “Information Security and Privacy”. It maintains affiliations with several Bosch internal IT departments and various external communities such as the Cyber Security Sharing and Analytics (CSSA) association and CERT-Verbund. Internationally, we are affiliated with the European TF-CSIRT, and globally, we are part of the FIRST community.

3.4. Authority

The establishment of the Bosch CERT was mandated by C/CY as described in Central Directive *Corporate Department for Cybersecurity*. Bosch CERT is authorized to order mandatory measures to resolve security incidents and vulnerabilities, and may appeal to its superior units and/or C/ISP to exert their authority, direct and indirect as necessary. Bosch CERT operates on the following Internet IP addresses: Bosch Internet IP Address Ranges

4. Policies

4.1. Types of Incidents and Level of Support

Bosch CERT is authorized to address all types of cybersecurity incidents which occur, or threaten to occur in our constituency and which require cross-organizational coordination. The level of support given by Bosch CERT will vary depending on the type and severity of the cybersecurity incident or issue, the type of constituent, the size of the user community affected, and our resources at the time. Incidents will be prioritized according to their apparent severity and extent.

Bosch CERT handles the following incident categories:

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusions
- Availability (impairment)
- Information Content Security
- Fraud
- Vulnerabilities

Bosch CERT is committed to keeping its constituency informed of potential vulnerabilities, and, where possible, will inform this community of such vulnerabilities before they are actively exploited. Product-specific advisories are internally available via an interactive web portal for user subscription.

4.2. Co-operation, Interaction and Disclosure of Information

Bosch CERT highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, and also with other internal and external parties which may contribute towards or make use of their services. Bosch CERT operates within the confines imposed by national and international legislation and relevant regulations and policies within the Bosch group. Bosch CERT promotes the controlled information exchange via the so called Traffic Light Protocol (TLP).

4.3. Communication and Authentication

Bosch CERT protects sensitive information in accordance with relevant legislation, regulations and policies within the Bosch group. Communication security (encryption and authentication) is currently achieved by S/MIME based email encryption

5. Services

5.1. Reactive Services

These services aim at the coordination of response to cybersecurity incidents within Bosch's constituency, in cooperation with the owners and providers of impacted parts of the the respective IT infrastructure, the national and international communities of

Computer Emergency Response Teams, telecommunication operators, internet service providers and other public and private bodies (police, investigators, courts) as appropriate.

5.1.1 Incident Management

The service provides Cybersecurity Incident Response for the Bosch Group as defined in CD02900 and CD09000. It is triggered by any cybersecurity event that is reported to C/CYT-IR. This can be based on a report to Bosch CERT via web form or via email, a report from our Cyber Threat Intelligence (CTI) team, a security event that is triggered from our monitoring or any other way in which we get aware of a possible breach of confidentiality, integrity, or availability (CIA) of an IT system.

5.1.2 Forensic Analysis

By retrospective analysis of artifacts, determine / explain what happened when (timeline) to foster further investigation or explain already seen effects / already found artifacts. For example, this includes forensic analyses of IT systems on-premise or of cloud systems, forensic analysis of embedded systems or forensic analysis of embedded systems of mobile devices and apps.

In addition, Bosch CERT will collect statistics concerning incidents which occur within or involve the Bosch community, and will notify the community as necessary to assist it in protecting against known attacks. To make use of Bosch CERT's incident response services, please send e-mail as per section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2. Proactive Activities

Beyond these reactive services, which engage after a cybersecurity incident has occurred, we also offer numerous proactive services. The objective of these services is to minimize the probability of a security incident or mitigate its potential impact.

5.2.1 Attack Simulation

During Attack Simulations cyber attacks against Bosch Systems are simulated using methods of real-world cyber criminals. These simulations can happen in collaboration with incident responders and service operators (Purple Teaming Exercises) or without their knowledge (Red Teaming Exercises). They serve the purpose of testing the efficiency of the established security measures and processes at Bosch and increase the cybersecurity resilience.

5.2.2 Fire Drill

The Cybersecurity Fire Drills practice crisis processes on the basis of simulated cyber attacks in order to prepare the crisis teams and other roles involved in the best possible way for real cyber attacks to support business continuity and to prevent damage to the company.

5.2.3 Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) supports stakeholders by providing actionable, evidence-based knowledge for cyber defense. This involves continuously identifying and assessing the threat landscape and attack techniques. Knowledge/intelligence is provided to stakeholders either proactively - based on assessments or in the form of support during incidents - or in response to a Request for Information.

5.2.4 Threat Control Management (incl. Security Control Engineering)

Threat Control Management provides an end-to-end process to address new threats. This involves an assessment and documentation of these threats in the form of adversarial behaviors (Procedures) as well as the prioritization for the Security Control Engineering process, which provides development of Security Controls for detection and prevention.

5.2.5 Awareness & Training (Learning)

The awareness and training topics focus on educating employees about cybersecurity threats and best practices. This is done by combining different training formats, phishing simulations and other events and communication activities. Mandatory trainings are delivered annually, with specific sessions offered regularly, and progress tracked via a Learning Management System. Success is measured by completion rates and employee feedback. The effectiveness of quarterly global phishing simulations is assessed by reporting rates, click rates and compromise rates. Event activities are conducted either in person or online on an as-needed basis.

5.2.6 Vulnerability Management Services

This service consists of several sub-services like holistic vulnerability management process within Bosch (E2E), active vulnerability scanning and vulnerability analysis service (check in external databases for new vulnerabilities and assess the situation for Bosch and provide advisories). In addition the Bosch PSIRT (Product Security Incident and Response Team) is part of the overall vulnerability management services.

6. Cybersecurity Incident Reporting Forms

For internal incidents, there ways to report are clearly defined. For externals there is no report form available, please use the contact possibilities mentioned in chapter 2 of this document.

7. Disclaimers

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