KIT CERT

Description as per RFC 2350

Contents

1 Information about this document **3**
- 1.1 Version History . . . 3
- 1.2 Distribution List for Notifications . . . 3
- 1.3 Locations where this Document may be found . . . 3
- 1.4 Document Authenticity . . . 3

2 Contact Information **3**
- 2.1 Name of the Team . . . 3
- 2.2 Address . . . 3
- 2.3 Date of Establishment . . . 4
- 2.4 Timezone . . . 4
- 2.5 Telephone Number . . . 4
- 2.6 Other Telecommunications . . . 4
- 2.7 Mail . . . 4
- 2.8 Public Keys and Encryption Information . . . 4
  - 2.8.1 PGP Key . . . 4
  - 2.8.2 S-MIME Certificate . . . 4
- 2.9 Team Members . . . 4
- 2.10 Other Information . . . 5
- 2.11 Points of Customer Contact . . . 5

3 Mandate **5**
- 3.1 Constituency . . . 5
  - 3.1.1 Clients . . . 5
  - 3.1.2 Networks . . . 5
  - 3.1.3 Domains . . . 6
  - 3.1.4 Autonomous Systems . . . 6
- 3.2 Authority . . . 6

4 Service Description **6**
- 4.1 Service Area: Information Security Event Management . . . 6
- 4.2 Service Area: Information Security Incident Management . . . 6
- 4.3 Service Area: Vulnerability Management . . . 6
- 4.4 Service Area: Situational Awareness . . . 7
- 4.5 Service Area: Knowledge Transfer . . . 7

5 Service Level Description **7**
- 5.1 Reaction Time . . . 7
- 5.2 Types of Incidents and Level of Support . . . 7
- 5.3 Co-operation, Interaction and Disclosure of Information . . . 7
  - 5.3.1 Communication and Authentication . . . 7

6 Incident Classification **8**

7 Integration in Existing CSIRT Systems **8**

1 Information about this document

This document contains a description of KIT-CERT according to RFC 2350. It provides information about the CERT, how to contact the team, and it describes its responsibilities and the services offered by KIT-CERT.

1.1 Version History

The current version is d7b4651. It was published on 2023-12-12.

Date	Description
2024-02-09	Restored version history of old document
2023-12-12	Update name of SCC[4]
2023-07-28	Complete rewrite of the this document
2017-02-14	Updated team member information; minor layout changes; fixed notation inconsistency
2013-10-17	Updated team member information; unified IPv6 address notation; spelling corrections
2013-03-06	Network list updates; URL updates; spelling corrections; minor additions
2012-11-07	Initial publication of this document

1.2 Distribution List for Notifications

None

1.3 Locations where this Document may be found

The current version of this document can be found at:

https://www.cert.kit.edu/p/rfc2350

1.4 Document Authenticity

This document can be retrieved from our webserver using TLS/SSL.

2 Contact Information

2.1 Name of the Team

KIT-CERT

2.2 Address

```
KIT-CERT
Karlsruhe Institute of Technology
```

Scientific Computing Center
76128 Karlsruhe
Germany

2.3 Date of Establishment

KIT-CERT was established March, 14th 2008.

2.4 Timezone

Europe/Berlin (UTC+01, and UTC+02 on DST).

2.5 Telephone Number

+49 721 608-45678

2.6 Other Telecommunications

Not available

2.7 Mail

cert@kit.edu

2.8 Public Keys and Encryption Information

2.8.1 PGP Key

Please obtain the PGP key using web key discovery (WKD). Key ID is: `0x6A2D8E94DCAD110A`, fingerprint is: `B7AB 809E 9D02 13E7 5B8F  141D 6A2D 8E94 DCAD 110A`

2.8.2 S-MIME Certificate

Find the latest certificate at: https://www.cert.kit.edu/p/smime.pem

2.9 Team Members

List of team members:

- Reese, Heiko
- Zangerle, Konstantin
- Oettig, Petter
- Tüllmann, Thorsten

2.10 Other Information

General information about the KIT-CERT as well as links to various recommended security resources can be found at: https://cert.kit.edu

2.11 Points of Customer Contact

The preferred method for contacting the KIT-CERT is via e-mail through cert@kit.edu; e-mail sent to this address will be delivered to the on-duty staff. If urgent assistance is required, include the keyword `[URGENT]` in your subject line.

If it is not possible or not advisable for security reasons to contact the KIT-CERT via e-mail, contact may be made by telephone during regular office hours.

The KIT-CERT hours of operation are generally restricted to regular business hours (09:00–17:00 local time, Monday through Friday, except on holidays).

3 Mandate

Mandate is documented in "IT-Sicherheitskonzept für das KIT"[2] and in "IT-Sicherheitsleitlinie"[3]. It is determined by the highest governing body of the KIT, the KIT Präsidium. The KIT-CERT is mandated as central coordination center for information security incidents and is the dedicated contact point for law enforcement agencies.

3.1 Constituency

3.1.1 Clients

The KIT-CERT constituency is the Karlsruhe Institute of Technology community (Mitglieder und Angehörige des KIT) and guests and partners (Gäste und Partner).

3.1.2 Networks

KIT-CERT will operate on the following public IPv4 networks:

- 129.13.0.0/16
- 141.3.0.0/16
- 141.52.0.0/16
- 157.180.228.0/22
- 157.180.232.0/22
- 192.108.45.0/24
- 192.108.46.0/24
- 192.108.47.0/24
- 192.108.68.0/24
- 193.174.1.192/29
- 193.196.32.0/20

KIT-CERT will operate on the following IPv6 networks:

- 2001:638:304::/48

- 2001:7c0:409::/48
- 2a00:1398::/29

KIT-CERT will also operate on various private networks operated by the KIT.

3.1.3 Domains

KIT-CERT will operate on every domain registered by KIT, foremost on the domain *kit.edu*.

3.1.4 Autonomous Systems

KIT-CERT is assigned to the autonomous system AS34878.

3.2 Authority

KIT-CERT is an organizational part of the Scientific Computing Center (SCC), but is the designated coordination center for all computer security incidents at KIT.

4 Service Description

Note: This description is based on the FIRST CSIRT Services Framework, Version 2.1[1]

4.1 Service Area: Information Security Event Management

- Monitoring & Detection
- Detection of successful Phishing
- Misbehaving accounts
- Mailfiltering
- Malware detection

4.2 Service Area: Information Security Incident Management

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Information Security Incident Coordination
- Crisis Management Support

4.3 Service Area: Vulnerability Management

- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

4.4 Service Area: Situational Awareness

- Analysis and Synthesis
- Communication

4.5 Service Area: Knowledge Transfer

- Training and Education for system administrators at KIT
- Talks & Presentations
- Technical and Policy Advisory

5 Service Level Description

5.1 Reaction Time

For the services **Information Security Incident Report Acceptance** and **Vulnerability Report Intake** we provide an initial reaction within 1 business day. All other services are provided on a best-effort basis.

5.2 Types of Incidents and Level of Support

KIT-CERT addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident, the amount of affected institutions within our constituency, and our resources at the time.

Note that no direct support will be given to end users in our constituency; they are expected to contact their respective system administrators, network administrators, or department heads for assistance. KIT-CERT will provide support to the latter group of persons.

5.3 Co-operation, Interaction and Disclosure of Information

KIT-CERT will exchange all necessary information with other CSIRTs as well as with other affected parties if they are involved in the incident or incident response process.

All information concerning one or more incidents passed on to other incident response teams, which include details about persons, organizations, IP-addresses, domain-names as well as other information revealing the identity of persons or organizations is anonymized unless explicitly stated otherwise by the persons or organizations in question. No information at all about any incident or vulnerability is given to other persons. German law enforcement personnel requesting information in the course of a criminal investigation is given the requested information within the limits of the court order and the criminal investigation, if they present a valid court order from a German court.

5.3.1 Communication and Authentication

All e-mail postings containing official statements on behalf of the team or team members should be signed using X.509 or PGP. All e-mail containing confidential information should be

encrypted and signed using X.509 or PGP. Information received in encrypted form should not be stored permanently in unencrypted form.

For sensitive information we prefer to use encrypted e-mail. For other communication phone, facsimile, postal service, or unencrypted e-mail may be used.

KIT-CERT supports the Traffic Light Protocol (TLP)

6 Incident Classification

We use the following criteria as guidance for prioritization of incoming incidents, loosely ordered by priority:

- Physical Safety of human beings
- Impact on KIT as a whole
- Impact on individual constituents
- Reputational Damage

7 Integration in Existing CSIRT Systems

We are members of:

- EDUCV, a working group of CERTs in the german higher education sector
- CERT-Verbund, a network of CERTs in germany
- Trusted Introducer, a european network of CSIRTs and CERTs
- FIRST, a global network of CSIRTs and CERTs

We strive to attend meetings and workshops of these communities.

References

[1] FIRST. *FIRST CSIRT Services Framework, Version 2.1*. URL: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1.

[2] *IT-Sicherheitskonzept des KIT*. URL: https://www.cert.kit.edu/p/itsec-konzept.

[3] *IT-Sicherheitsleitlinie des KIT*. URL: https://www.cert.kit.edu/p/itsec-leitlinie.

[4] Public Relations Office of Karlsruhe Institute of Technology. *KIT Renames Information Technology Center*. URL: https://www.kit.edu/kit/english/pi_2023_092_kit-renames-information-technology-center.php.