CERT@tue

Established according to RFC-2350

1. Document Information

1.1. Date of Last Update
This is version 1.4 of August 27th 2019.

1.2. Distribution List for Notifications
Any specific questions or remarks please address to the CERT@tue.nl mail address.

1.3. Locations where this Document May Be Found
The current version of this profile is always available on:
https://www.tue.nl/universiteit/over-de-universiteit/organisatie/diensten/ict-services/ict-security/

2. Contact Information

2.1. Name of the Team
CERT@tue, the CSIRT or CERT team for the Eindhoven University of Technology (TU/e), The Netherlands.

2.2. Address
CERT@tue
ICT Services
P.O. Box 513
NL – 5600 MB Eindhoven
The Netherlands

2.3. Time Zone
GMT+1 (GMT+2 with DST, according to EC rules)

2.4. Telephone Number
+31 (0)40 247 5678 (during office hours only)

2.5. Facsimile Number
Not available.

2.6. Other Telecommunication
Not available.

2.7. Electronic Mail Address
CERT@tue.nl
2.8. Public Keys and Encryption Information
CERT@tue uses pgp for secure communication.
We generate once a year a new key for the email address CERT@tue.nl
Key information:
Name: TUECERT
ID: 0x/51CCCCF6
Fingerprint: 1DD2 125B 0C33 28FD 3B87 D1CC 6805 BF70 51CC CCF6
Valid until 4/1/2021
http://pgp.surfnet.nl/pks/lookup?op=vindex&fingerprint=on&search=CERT@tue

2.9. Team Members
CERT@tue team members are drawn from the ranks of Eindhoven Universiteit ICT professionals.

2.10. Other Information
See https://www.tue.nl/universiteit/over-de-universiteit/organisatie/diensten/ict-services/ict-security/

CERT@tue is registered by SURFcert, see https://wiki.surfnet.nl/display/CSIRTs

2.11. Points of Customer Contact
Normal cases:
Use CERT@tue mail address.
Business hours response only: 0900-1600 local time on Monday-Friday save public holidays in The Netherlands.

EMERGENCY cases:
Use CERT@tue phone number with back-up of mail address for all detail (putting EMERGENCY in subject line is recommended). The CERT@tue phone number is available at office hours. Outside business hours the duty-officer will check the email address on a regular basis.

3. Charter

3.1. Mission Statement
CERT@tue’s mission is to coordinate the resolution of IT security incidents related to the Eindhoven University of Technology, and to help prevent such incidents from occurring.

For the world, CERT@tue is the TU/e interface with regards to IT security incident response. All IT security incidents (including abuse) related to TU/e can be reported to CERT@tue.

3.2. Constituency
Technische Universiteit Eindhoven (TU/e) or Eindhoven University of Technology, with all its organizations and employees.

3.3. Sponsorship and/or Affiliation
CERT@tue is part of TU/e operations.
3.4. Authority
CERT@tue coordinates security incidents on behalf of TU/e and has no authority reaching further than that. CERT@tue is however expected to make operational recommendations in the course of its work. Such recommendations can include for instance blocking addresses or networks. The implementation of such recommendations is not a responsibility of CERT@tue however, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support
All incidents are considered normal priority unless they are labeled EMERGENCY. CERT@tue itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT@tue as EMERGENCY, but it is up to CERT@tue to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information
ALL incoming information is handled confidentially by CERT@tue, regardless of its priority.

Information that is evidently very sensitive in nature is only communicated in an encrypted fashion (see 2.8 above). When reporting an incident of very sensitive nature, please state so explicitly (e.g. by using the label VERY SENSITIVE in the subject field of e-mail) and use encryption as well.

CERT@tue will use the information you provide to help solve security incidents, as all CSIRTs do or should do. This means explicitly that the information will be distributed further only on a need-to-know base, and in an anonymized fashion.

If you object to this default behavior of CERT@tue, please make explicit what CERT@tue can do with the information you provide. CERT@tue will adhere to your policy, but will also point out to you if that means that CERT@tue cannot act on the information provided.

CERT@tue does not report incidents to law enforcement, unless Dutch law requires so – as in the case of first-degree crime. Likewise, CERT@tue cooperates with law enforcement in the course of an official investigation only, meaning a court order is present, AND in case a CERT@tue constituent requests that CERT@tue cooperates in an investigation. In the latter case, when a court order is absent, CERT@tue will only provide information on a need-to-know base.

4.3. Communication and Authentication
See 2.8 above. Usage of encryption in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Incident Response (Triage, Coordination, Resolution)
CERT@tue is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). CERT@tue therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. CERT@tue will offer support and advice on request.

5.2. Proactive Activities
CERT@tue pro-actively advises its constituency with regards to recent vulnerabilities and trends in hacking/cracking.
CERT@tue advises TU/e on matters of computer and network security. It can do so pro-
actively in urgent cases, or on request.

Both roles are roles of consultancy – CERT@tue is not responsible for implementation.

6. Disclaimers

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