TNOCert profile

Established according to RFC-2350.

1. Document information

1.1. Date of last update

This is version 0.3 of 1-12-2011.

1.2. Distribution list for notifications

This profile is kept up-to-date on the location specified in 1.3.
Email notification of updates are sent to:

- All TNOCert members
- SURFcert (see http://www.surfnet.nl/nl/Thema/surfcert/Pages/Default.aspx)

Any questions about updates please address to the TNOCert email address.

1.3. Locations where this document may be found

The current version of this profile is always available on http://www.tno.nl/cert

2. Contact information

2.1. Name of the team

Full name: TNO IT Security Coordination
Short name: TNOCert
TNOCert is the CERT or CSIRT team for TNO in the Netherlands.

2.2. Address

TNO
Information Services
IT Security Coordinator
P.O.Box 6014
2600 JA Delft
The Netherlands

2.3. Time zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone number

+31 88 8667100

2.5. Facsimile number

Not available.

2.6. Other telecommunication

Not available.

2.7. Electronic mail address

Organisatie-TNO-ITSecurity@tno.nl

This address can be used to report all security incidents related to the TNOCert constituency, including copyright issues, spam and abuse.

2.8. Public keys and encryption information
Currently no encrypted email is supported.

2.9. Team members
No information is provided about the TNOCert team members in public.

2.10. Other information
TNOCert is registered by SURFcert, see
http://www.surfnet.nl/nl/Thema/surfcert/teams/Pages/CERTteams.aspx .

2.11. Points of customer contact
Regular cases: use TNOCert email address.
Regular response hours: Monday-Friday, 09:00-17:00 (except public holidays in the Netherlands).
EMERGENCY cases: send email with EMERGENCY in the subject line.

3. Charter

3.1. Mission statement
The mission of TNOCert is to co-ordinate the resolution of IT security incidents related to the constituency (see 3.2), and to help prevent such incidents from occurring.

3.2. Constituency
The constituency for TNOCert is TNO in the Netherlands.
This constituency consists of:

- Netherlands Organisation for Applied Scientific Research TNO
- At least the domain: tno.nl
- The following IP ranges: 134.221.0.0/16, 139.63.0.0/16, 192.43.212.0/24, 192.87.96.0/24, 192.87.168.0/24, 195.169.92.0/24

3.3. Sponsorship and/or affiliation
TNOCert is part of Netherlands Organisation for Applied Scientific Research TNO.

3.4. Authority
The team coordinates security incidents on behalf of the constituency and has no authority reaching further than that. The team is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not a responsibility of the team, 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.

An incident can be reported to TNOCert as EMERGENCY, but it is up to TNOCert 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 TNOCert, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of the email.

TNOCert supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

TNOCert will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties, but only on a need-to-know base and preferably in an anonymised fashion.

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

TNOCert only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that TNOCert cooperates in an investigation. When a court order is absent, TNOCert will only provide information on a need-to-know base.

4.3. Communication and authentication

See 2.8 above. In cases where there is doubt about the authenticity of information or its source, TNOCert reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident response (triage, coordination and resolution)

TNOCert is responsible for the coordination of security incidents somehow involving the constituency (as defined in 3.2). TNOCert therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency, however TNOCert will offer support and advice on request.

5.2. Proactive activities

TNOCert pro-actively advises the constituency in regard to recent vulnerabilities and trends in hacking/cracking.
TNOCert advises the constituency 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: TNOCert is not responsible for implementation.

6. Incident reporting forms

Not available. Preferably report in plain text using email or use the phone.

7. Disclaimers

TNO generic disclaimer concerning email communication is available here: http://www.tno.nl/emaildisclaimer.