CERT Open Universiteit profile

Established according to RFC-2350.

- 1. Document Information
  - 1.1. Date of Last Update
  - 1.2. Distribution List for Notifications
  - 1.3. Locations where this Document May Be Found
- 2. Contact Information
  - 2.1. Name of the Team
  - 2.2. Address
  - 2.3. Time Zone
  - 2.4. Telephone Number
  - 2.5. Facsimile Number
  - 2.6. Other Telecommunication
  - 2.7. Electronic Mail Address
  - 2.8. Public Keys and Encryption Information
  - 2.9. Team Members
  - 2.10. Other Information
  - 2.11. Points of Customer Contact
- 3. Charter
  - 3.1. Mission Statement
  - 3.2. Constituency
  - 3.3. Sponsorship and/or Affiliation
  - 3.4. Authority
- 4. Policies
  - 4.1. Types of Incidents and Level of Support
  - 4.2. Co-operation, Interaction and Disclosure of Information
  - 4.3. Communication and Authentication
- 5. Services
  - 5.1. Incident Response (Triage, Coordination and Resolution)
  - 5.2. Proactive Activities
- 6. Incident reporting Forms
- 7. Disclaimers

1. Document Information

1.1. Date of Last Update

This is version 5 of 14-02-2023.

1.2. Distribution List for Notifications

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

- All CERT OU members
- SURFcert (e-mail: cert AT surfcert DOT nl , more information see SURFcert's TI Page or RIPE Information)

Any questions about updates please address to the CERT OU e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on www.ou.nl/security .

2. Contact Information

2.1. Name of the Team

Full name: CERT Open Universiteit
Short name: CERT OU
CERT OU is the CERT team for the Open University of The Netherlands .

2.2. Address

Open Universiteit
T.a.v. CERT OU
Postbus 2960
6401 DL Heerlen
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST, according to EC rules)

2.4. Telephone Number

+31 (0)45 5762306

2.5. Facsimile Number

CERT Open Universiteit can NOT be contacted by Facsimile.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

cert@ou.nl
This address can be used to report all security incidents which relate to the CERT OU constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

Encryption for secure communication is NOT supported .

2.9. Team Members

No information is provided about the CERT OU team members in public.

2.10. Other Information

- CERT OU is registered by SURFcert, see https://wiki.surfnet.nl/display/CSIRTS .

2.11. Points of Customer Contact

Regular cases: use CERT OU e-mail address.
Regular response hours: Monday-Friday, 08:30-17:00 (except public holidays in The Netherlands).
EMERGENCY cases: send e-mail with EMERGENCY in the subject line.

3. Charter

3.1. Mission Statement

The mission of CERT OU is to co-ordinate the resolution of IT security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring.
All IT security incidents (including abuse) related to the domain ou.nl can be reported to CERT OU.

3.2. Constituency

The constituency for CERT OU is the Open Universiteit in The Netherlands .
This constituency consists of:

- Employees and hired staff of the Open Universiteit and its affiliate institutions.
- Students and guests of the university if and when they use a computer with an IP-adress in the range that is controlled by the university.
  The Open Universiteit controlls the IPv4 range 145.20.*.* and IPv6 range 2001:610:338::/48

3.3. Sponsorship and/or Affiliation

CERT OU is part of the Dutch distance teaching university named Open Universiteit .

3.4. Authority

The team coordinates security incidents on behalf of their 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. CERT OU itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT OU as EMERGENCY, but it is up to CERT OU to decide whether or not to uphold that status.

4.2. Cooperation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by CERT OU, regardless of its priority.

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

CERT OU supports the Information Sharing Traffic Light Protocol (ISTLP - see http://www.surf.nl/diensten-en-producten/surfcert/information-sharing-traffic-light-protocol/index.html) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT OU 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 CERT OU, please make explicit what CERT OU can do with the information you provide. CERT OU will adhere to your policy, but will also point out to you if that means that CERT OU cannot act on the information provided.

CERT OU does not report incidents to law enforcement, unless national law requires so. Likewise, CERT OU 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 CERT OU cooperates in an investigation. When a court order is absent, CERT OU will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. PGP/GnuPG is NOT currently supported. In all cases where highly sensitive information is involved, you are recommended to contact CERT OU by phone or in person on site. If needed, a method of communication will then be established which satisfies the security demands on both sides.
In cases where there is doubt about the authenticity of information or its source, CERT OU reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

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

5.2. Proactive Activities

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

6. Incident reporting Forms

Not available. Preferably report in plain text using e-mail - or use the phone.

7. Disclaimers

None.