CERT-UU RFC 2350

Expectations for Computer Security Incident Response, filled in for Utrecht University

January 22, 2024

Contents

Document information

This document contains a description of CERT-UU in accordance with RFC 2350 “Expectations for Computer Security Incident Response”. It provides basic information about CERT-UU, its channels of communication, and its roles and responsibilities.

Date of last update

January 22, 2024

Distribution list for updates

There is no distribution list for updates to this document.

Location of this document

The current version of this document is available via https://www.uu.nl/cert

Contact information

Name of the team

“CERT-UU”: the Computer Emergency Response Team of Utrecht University.

Mailing address

Universiteit Utrecht

Directie Information and Technology Services

T.a.v. CERT-UU

Heidelberglaan 8

Postbus 80.125

3508 TC Utrecht

The Netherlands

Time zone

CERT-UU lives in timezone ’Europe/Amsterdam’ which means CET (UTC+1) in winter and CEST (UTC+2) in the summer.

Telephone number

Only for emergencies that require direct attention. Will be forwarded to the mobile phone of the CERT-UU member on duty after a short announcement.

+31-30-2535959

Facsimile number

Fax is not supported for communicating with CERT-UU.

Electronic mail address

cert@uu.nl

Public keys and encryption

CERT-UU uses PGP/gpg for secure communications. Our public PGP/gpg key is available on the public keyservers.

We generate a new key at the beginning of each year, valid for that year, for the e-mail address cert@uu.nl and sign it with our cert-uu master key:

```
pub rsa4096/0xAB03508032FD74D9 2022-02-17 [SC]

B0FE8E9B381A919DAE5AD1E5AB03508032FD74D9

uid [ full ] CERT-UU Masterkey

sub rsa4096/0x477AE3C8C8B61F2D 2022-02-17 [E]
```

The year key will be available via the keyserver pgp.surfnet.nl and via the website https://www.uu.nl/cert.

Team Members

The members of CERT-UU are:

- Koos van den Hout
- Simon Kort
- Dennis Swanink
- Johnny Baas
- Chris Konings
- Peter Schmitt
- Gitte Groeneveld
- Lukas de Groen
- Bert Oostland
- Hans van der Made

The chairpersons of CERT-UU are:

- Koos van den Hout
- Chris Konings

The CISO responsible for information security at Utrecht University is:

- David de Boer

Operating hours

CERT-UU is reachable 7 days per week from 08:00 until 22:00 local time (CET/CEST) by phone. CERT-UU will regularly read e-mail messages 7 days per week from 08:00 until 20:00 local time.

Additional contact information

None

Charter

Mission statement

The UU ”Computer Emergency Response Team” (CERT-UU) has been set up to manage incidents which Utrecht University can be confronted with in the areas of information security.

CERT-UU is primarily active in the coordination of prevention, detection and resolution of security incidents.

Constituency

UU meaning Utrecht University.

Systems, networks and applications part of the UU computing and communications infrastructure, including those managed by third parties and third-party infrastructure managed by the UU.

Sponsoring organization

CERT-UU is overseen by the CISO who is accountable to the Utrecht University board of directors.

Authority

CERT-UU has the authority to take all necessary steps to prevent increasing damage, including the authority to disconnect a system from the network pending investigation.

Policies

Types of incidents and level of support

CERT-UU will usually respond within one working day. All incidents are considered normal priority unless labeled EMERGENCY. CERT-UU itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT-UU as EMERGENCY but it is up to CERT-UU to decide whether or not to uphold that status. When information is received by CERT-UU about vulnerabilities which create risks for future incidents, CERT-UU may decide to act upon this information

Co-operation, Interaction and Disclosure of Information

CERT-UU adheres to the Traffic Light Protocol as described at https://www.first.org/tlp/. All incoming information is handled confidentially by CERT-UU, regardless of its priority. Information that is evidently very sensitive in nature is only communicated in encrypted format. When reporting an incident of very sensitive nature, please state so explicitly (by using the [TLP:RED] label or the label VERY SENSITIVE in the subject field of e-mail) and use encryption as well.

CERT-UU 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 basis, and in anonymized fashion.

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

CERT-UU does not report incidents to law enforcement, unless Dutch law requires us to. We may advise owners of systems to report serious incidents to law enforcement. CERT-UU cooperates with law enforcement in the course of an official investigation only.

CERT-UU will interact about incidents with upstream CSIRTs such as the SURFcert team.

CERT-UU does not deal with the press directly. All press-enquiries will have to go via the communications office of the Utrecht University.

Communication and authentication

We highly recommend using PGP/gpg to encrypt information send to us via e-mail. We will use PGP/gpg whenever possible and sending us PGP/gpg signed and/or encrypted e-mail is seen as an invitation to use PGP/gpg signing and encryption on return e-mail.

We may also ask for verification such as return phone numbers when communicating via telephone.

Services

Incident response

Incident triage

Incident triage is handled by CERT-UU.

Incident coordination

Incident coordination is handled by CERT-UU.

Incident resolution

Incident resolution is left to the responsible owner of the related information processing facility.

Proactive activities

CERT-UU proactively advises its constituency with regards to recent vulnerabilities and trends in attacks. CERT-UU advises Utrecht University on matters of computer and network security. It can do so unrequested and requested.

Incident reporting forms

CERT-UU does not use incident reporting forms at this time.

Disclaimer

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