Radboud Universiteit

RFC-2350

Following profile of CERT-RU has been established in adherence to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version 1.2 of February 20 2014.

1.2. Distribution List for Notifications

The current version of this profile is always available on:
http://www.ru.nl/cert/.
Only RU DSC's (Domain Security Contacts) are actively notified of updates to this framework. Any specific questions or remarks please address to the CERT-RU mailaddress.

1.3. Locations where this Document May Be Found

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

2. Contact Information

2.1. Name of the Team

CERT-RU, the CSIRT or CERT team for the Radboud University of Nijmegen (RU), The Netherlands.

2.2. Address

CERT-RU
IT Service Centre
P.O.Box 9101
NL - 6500 HB Nijmegen
The Netherlands

2.3. Time Zone

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

2.4. Telephone Number

+31 (0)24 361 0818

2.5. Facsimile Number

+31 (0)24 3617804

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

cert@ru.nl

2.8. Public Keys and Encryption Information

Only PGP is currently supported for secure communication.
The CERT-RU public PGP key is available on the public keyservers.
Its key-id is 0x6FC5001A and its fingerprint is
F8FA 4E92 382D F76A 6455 A51B D9BA 0496 6FC5 001A.
Please use this key to encrypt messages sent to CERT-RU. Sign your message using your own key please – it helps if that key is verifiable using the public keyservers.
Messages from CERT-RU will in due cases be signed using the same CERT-RU key. Its credentials can be checked by you on the public keyservers.

2.9. Team Members

CERT-RU team members are drawn from the ranks of RU ICT professionals. Further details to be found at http://www.ru.nl/cert/

2.10. Other Information

See http://www.ru.nl/cert/

2.11. Points of Customer Contact

Normal cases:
Use CERT-RU mailaddress.
Business hours response only: 0900-1700 local time on Monday-Friday save public holidays in The Netherlands.
EMERGENCY cases:
Use CERT-RU phonenumber with back-up of mailaddress for all detail (putting EMERGENCY in subject line is recommended). The CERT-RU phonenumber is available at all times. Outside business hours the duty-officer(not a CERT-RU team member) decides if CERT-RU will be involved directly or not.

3. Charter

3.1. Mission Statement

CERT-RU's mission is to coordinate the resolution of IT security incidents related to the Radboud University of Nijmegen (RU) , and to help prevent such incidents from occurring.
For the world, CERT-RU is the RU interface with regards to IT security incident response. All IT security incidents (including abuse) related to RU can be reported to CERT-RU.

3.2. Constituency

Radboud Universiteit Nijmegen (RU) or Nijmegen University, with all its organizations, employees and students.

3.3. Sponsorship and/or Affiliation

CERT-RU is part of RU operations.

3.4. Authority

CERT-RU coordinates security incidents on behalf of RU and has no authority reaching further than that. CERT-RU is however expected to make operational recommendations in the course of its work. The implementation of such recommendations is not a responsibility of CERT-RU however, but solely of those to whom the recommendations were made. CERT-RU has the authority to block addresses or networks.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. CERT-RU itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT-RU as EMERGENCY, but it is up to CERT-RU 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-RU, regardless of its priority.
Information that is evidently very sensitive in nature is only communicated in an encrypted fashion. 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-RU 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 behaviour of CERT-RU, please make explicit what CERT-RU can do with the information you provide. CERT-RU will adhere to your policy, but will also point out to you if that means that CERT-RU cannot act on the information provided.
CERT-RU does not report incidents to law enforcement, unless Dutch law requires so – as in the case of first-degree crime. Likewise, CERT-RU cooperates with law enforcement in the course of an official investigation only, meaning a court order is present, AND in case a CERT-RU constituent requests that CERT-RU cooperates in an investigation. In the latter case, when a court order is absent, CERT-RU will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Incident Response

5.1.1. Incident Triage

5.1.2. Incident Coordination

5.1.3. Incident Resolution

CERT-RU is responsible for the the coordination of security incidents somehow involving RU. CERT-RU therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within RU and externally.

5.2. Proactive Activities

CERT-RU pro-actively advises its constituency with regards to recent vulnerabilities and trends in hacking/cracking.
CERT-RU advises RU 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-RU is not responsible for

implementation.

6. Incident Reporting Forms

Not available.

7. Disclaimers

Not available