RFC2350 CSIRT-KNAW

(Computer Security Incident Response Team for the Royal Netherlands Academy of Arts and Sciences)

(Zoektermen: cert, csirt, information, security, incident, response, team, KNAW, knaw, abuse, cert-knaw, knaw-cert, csirt-knaw, knaw-csirt)

1 Document Information

1.1 Date of last update

This is version 0.1 January 22nd 2008

1.2 Distribution list for notifications

The current version of this document can be found at www.knaw.nl/security/rfc2350-csirt-knaw.pdf
This document will not actively be distributed.

1.3 Locations where this document may be found

The current version of this document can be found at www.knaw.nl/security/csirt/rfc2350_csirt-knaw.pdf

2 Contact Information

2.1 Name of the team

The name of the team is CSIRT-KNAW

2.2 Address

CSIRT-KNAW
P.O. Box 19121
1000 GC Amsterdam
The Netherlands

2.3 Time Zone

GMT+1;GMT+2 with DST according to EC rules

2.4 Telephone number

Not yet available

2.5 Facsimile number

+31 20 6204941

2.6 Other telecommunication

Not available

2.7 Electronic mail address

CSIRT@knaw.nl

2.8 Public keys and encryption information

Not yet available

2.9 Team members

The CSIRT-KNAW team members are recruited from the IT-professionals within the KNAW

2.10 Other information

Not available

2.11 Points of customer contact

Normal cases: CSIRT@knaw.nl Business hours (8.30 – 17.30, Monday-Friday excluding public holidays), response within 24 hours
Emergency: Call +31 6 12933184 and send an e-mail stating detailed information to CSIRT@knaw.nl. Start the subject field with "EMERGENCY". Emergency incidents (at the discretion of the CSIRT) get immediate attention during business hours. Outside business hours emergency calls are treated with "best effort", depending on availability of members of the CSIRT.

3 Charter

3.1 Mission statement

The mission of the CSIRT-KNAW is to coordinate the resolution of information security incidents related to the KNAW and to help the prevention and detection of such incidents.
All information security incidents related to the KNAW can be reported to CSIRT-KNAW.

3.2 Constituency

KNAW (Royal Netherlands Academy of Arts and Sciences), including all its institutes, its employees and other users of its ICT infrastructure.
Internet domains: knaw.nl

3.3 Sponsorship and/or affiliation

CSIRT-KNAW is part of the KNAW operations

3.4 Authority

CSIRT-KNAW registers information security incidents and coordinates the resolution of all incidents related to the KNAW. CSIRT-KNAW may offer advice on the resolution of the incidents and how to prevent those incidents in the future. The implementation of those recommendations is not within the authority and therefore not a responsibility of the CSIRT-team.

4 Policies

4.1 Types of incidents and level of support

Normal cases: Business hours (8.30 – 17.30, Monday-Friday excluding public holidays), response within 24 hours
Emergency cases: At the discretion of the CSIRT, get immediate attention during business hours. Outside business hours emergency calls are treated on basis "best effort", depending on availability of members of the CSIRT.

4.2 Co-operation, interaction and disclosure of information

All incoming information is handled confidentially.
Highly confidential information is communicated with encryption.
All information is shared based on "need to know".
All members of the CSIRT are bound by a signed "non-disclosure agreement"
Information regarding incidents that may have legal consequences is shared with the legal advisor of the KNAW. The board of directors will decide if (and how) information should be shared with the Dutch law enforcement.

4.3 Communication and authentication

PGP for signing and encryption of e-mail messages is not yet implemented.

5 Services

5.1 Prevention

CSIRT-KNAW offers advise on information security related matters regarding the constituency. The implementation of these recommendations is at the discretion of the concerning management. The CSIRT-site will support end-users with "best practices" for information security.

5.2 Detection

Detection will probably mostly be triggered by incidents reported to the CSIRT. The CSIRT can use information of the intrusion detection and logging systems in use and managed by the corporate IT-support organization.

5.3 Resolution

The CSIRT will coordinate and trace the resolution of information security incidents. The CSIRT may offer advice on the resolution and prevention of incidents. Implementation and resolution of incidents resort under the authority of the concerning management.

5.4 Post processing

The CSIRT will track the resolution of incidents and will register incidents in its incident registration system for analysis and reporting purposes.

6 Incident reporting forms

None available

7 Disclaimers

-