HAN-CERT - RFC 2350
HAN_ University of Applied Sciences

Version: 1.5
Date: Sept 13, 2021

CONTENTS

1 Document Information

This document describes the profile (contact information, services, etc.) of HAN-CERT, the "Computer Emergency Response Team of the HAN University of Applied Sciences". The structure of this document is based on RFC 2350.

1.1   Date of Last Update

This is version 1.5, published on Sept 13, 2021.

1.2   Distribution List for Notifications

There is no distribution list for notifications.

1.3   Locations where this Document May Be Found

The current version of this document is available at https://www.hanuniversity.com

2 Contact Information

2.1 Name of the Team

"HAN-CERT": the Computer Emergency Response Team of the HAN University of Applied Sciences.

2.2 Address

HAN University of Applied Sciences
Secretariaat Services ICT, HAN-CERT
Ruitenberglaan 26
6826 CC Arnhem
The Netherlands

2.3 Time Zone

HAN-CERT uses local time. This means CET (UTC+1) in winter and CEST (UTC+2) in summer.

2.4 Telephone Number

+31 (0)24 353 05 00

2.5 Facsimile Number

Not available

2.6 Electronic Mail Address

cert@han.nl

2.7 Website Address

HAN-CERT doesn't have a website.

2.8 Public Keys and Encryption Information

HAN-CERT uses PGP for secure communication. Our public PGP key is available on the public keyservers (e.g. http://wwwkeys.pgp.net).

Key-id: 0x94A1B643

Fingerprint: E064 184F 943D 76C1 01F5 F170 5E47 76FB 94A1 B643

Please use this key to encrypt messages sent to HAN-CERT. Please sign your message using your own key. It helps if that key is verifiable using the public keyservers. Messages from HAN-CERT will always be signed using the HAN-CERT key. Its credentials can be checked by you on the public keyservers.

2.9 Team Members

The names of the members of HAN-CERT are available on request.

2.10 Operating Hours

HAN-CERT is open Mon-Fri from 8:30 to 17:00 CET/CEST. During weekend and holidays, the HAN-CERT mailbox is occasionally being monitored.

EMERGENCY cases:
Use HAN-CERT phone number with back-up of mail address for all detail (putting EMERGENCY in subject line is recommended).

3 Charter

3.1 Mission Statement

HAN-CERT's mission is:

- to coordinate the prevention and resolution of security incidents, related to the information processing facilities of the HAN, with the aim for increasing the confidentiality, integrity and availability of these facilities.

3.2 Constituency

HAN-CERT will provide services to the HAN. Security incidents can be reported by anyone, as long as they are related to the information processing facilities of the HAN.

3.3 Sponsorship and/or Affiliation

HAN-CERT is part of the HAN University of Applied Sciences.

3.4 Authority

If there is proof or suspicion of abuse of IT services, HAN-CERT is authorised to secure evidence and take measures to prevent future misuse.

4 Policies

4.1 Types of Incidents and Level of Support

HAN-CERT will usually respond within one working day. All incidents are considered normal priority unless they are labeled EMERGENCY. HAN-CERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to HAN-CERT as EMERGENCY, but it is up to HAN-CERT 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 HAN-CERT, 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.

HAN-CERT 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 anonymised fashion.

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

HAN-CERT will only involve the police, or provide sensitive information to third parties, when directed to do so by an authorised representative of HAN University of Applied Sciences.

4.3 Communication and Authentication

Usage of PGP in all cases where sensitive information is involved is highly recommended. See 2.9 above.

5 Services

5.1 Incident Response

5.1.1 Incident Triage
Incident triage is handled by HAN-CERT.

5.1.2 Incident Coordination
Incident coordination is handled by HAN-CERT.

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

5.2 Proactive Activities
HAN-CERT pro-actively advises its constituency with regards to recent vulnerabilities and trends in hacking/cracking. HAN-CERT advises HAN 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. HAN-CERT is not responsible for implementation.

6 Incident Reporting Forms
Reporting forms are not available.

7 Disclaimer
The information in this document is provided for information purposes only. The HAN makes no warranties about the accuracy or completeness of any information contained in this document. The HAN does not accept liability for any damages, losses or personal harm whatsoever, arising out of, or in any way related to, the use of this document.