HZ-CSIRT profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version **2.1 of June 10, 2016.**

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 **HZ-CSIRT** members
- All **HZ-CSIRT** constituents
- SURFcert (see https://www.surf.nl/diensten-en-producten/surfcert/index.html)

Any questions about updates please address to the **HZ-CSIRT** e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on **http://hz.nl/csirt**.

2. Contact Information

2.1. Name of the Team

Full name: **Computer Security Incident Response Team of HZ University of Applied Sciences**
Short name: **HZ-CSIRT**
HZ-CSIRT is the CSIRT team for **HZ University of Applied Sciences (HZ), The Netherlands** in **The Netherlands .**

2.2. Address

HZ University of Applied Sciences
HZ-CSIRT, Afd. Automatisering
P.O. Box 364
4380 AJ Vlissingen
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

+31 (0)118 489277 (Helpdesk)

2.5. Facsimile Number

+31 (0)118 489795 Note: this is not a secure fax.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

security@hzeeland.nl
This is a mail alias that relays mail to the human(s) on duty for the **HZ-CSIRT**. The address can be used to report all security incidents which relate to the **HZ-CSIRT** constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

The HZ-CSIRT has a PGP/GnuPG key, whose Key-ID is 0xDC899C3F and whose fingerprint is:
7D55 B928 638A CF17 6A41 2477 A0F6 67BC DC89 9C3F
Please use this key to encrypt messages sent to HZ-CSIRT. Sign your message using your own key please - it helps if that key is verifiable using the public key servers.

This key still has relatively few signatures; efforts are underway to increase the number of links to this key in the PGP "web of trust".

2.9. Team Members

HZ-CSIRT team members are drawn from the ranks of HZ ICT professionals
No information is provided about the **HZ-CSIRT** team members in public.

2.10. Other Information

- See the **HZ-CSIRT** webpages **http://hz.nl/csirt .**
- **HZ-CSIRT** is registered by SURFcert, see https://www.surf.nl/en/services-and-products/surfcert/csirts/csirts-registered-with-surfcert/index.html
- **HZ helpdesk** webpages http://helpdesk.hz.nl/

2.11. Points of Customer Contact

Regular cases: use **HZ-CSIRT** e-mail address.
Regular response hours: Monday-Friday, 09:00-17:00 (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 **HZ-CSIRT** is to resolve IT security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring.
For the world, **HZ-CSIRT** is the HZ interface with regards to IT security incident response. All IT security incidents (including abuse) related to HZ can be reported to **HZ-CSIRT**.

3.2. Constituency

The constituency for **HZ-CSIRT** is **HZ University of Applied Sciences (HZ)** in **The Netherlands .**
This constituency consists of:

- **HZ University of Applied Sciences (HZ) and institutions connected to HZ's network, with all related students and employees,**
- **Domain names: hz.nl and many other domain names registered by HZ,**
- **IP subnets: 145.19.0.0/16 (IPv4) 2001:610:300::/48 (IPv6).**

3.3. Sponsorship and/or Affiliation

HZ-CSIRT is part of **Dienst Informatievoorziening & Automatisering (DIA) of HZ University of Applied Sciences**.

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. **HZ-CSIRT** itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to **HZ-CSIRT** as EMERGENCY, but it is up to **HZ-CSIRT** 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 **HZ-CSIRT**, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. 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, and if possible using encryption as well.

HZ-CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

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

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

4.3. Communication and Authentication
See 2.8 above. Usage of PGP/GnuPG in all cases where sensitive information is involved is highly recommended. In cases where there is doubt about the authenticity of information or its source, **HZ-CSIRT** reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)
HZ-CSIRT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). **HZ-CSIRT** therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however **HZ-CSIRT** will offer support and advice on request.

5.2. Proactive Activities
HZ-CSIRT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.
HZ-CSIRT advises **HZ University of Applied Sciences** 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: **HZ-CSIRT** 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

A generic disclaimer stating confidentiality and “need to know”-status of specific information is available below. In due cases this disclaimer will be adopted according to the nature of the incident and persons/organizations involved.

```
-------------start generic disclaimer------------------
<addressee>,
You are receiving this information due to your involvement in an incident dealt with by HZ-CSIRT
(hz.nl/csirt). You must treat this information as strictly
confidential. Copies of this information in your possession (electronic and/or hard copy) must
be stored in a manner which is not accessible to unauthorised third parties. If it should be
necessary to further distribute this information in the process of handling the incident
involved, this should be done on an individual basis, making use of this disclaimer and with a
copy being sent to HZ-CSIRT.
-------------end generic disclaimer------------------
```