CSIRT Description for Z-CERT

Formatted according to RFC2350

1. About this document

1.1 Date of Last Update

This is version 2.0, published 06-Sep-2023.

1.2 Distribution List for Notifications

If you would like to receive updates of this document, please contact us at cert@z-cert.nl.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the public Z-CERT website; its URL is https://z-cert.nl/RFC2350-z-cert.pdf

Please make sure you are using the latest version.

2. Contact Information

2.1 Name of the Team

"Z-CERT", short for “Zorg-CERT”, the computer emergency response team for the healthcare sector in the Netherlands.

2.2 Address

Z-CERT
Stationsplein 121
3818 LE Amersfoort
The Netherlands

2.3 Time Zone

Europe/Amsterdam (GMT+0100, and GMT+0200 from the last weekend in March to the last weekend in October)

2.4 Telephone Number

+31-33-737-0609

2.5 Facsimile Number

None available

2.6 Other Telecommunication

None available

2.7 Electronic Mail Address

cert@z-cert.nl

2.8 Public Keys and Other Encryption Information

Z-CERT has a PGP key which is changed every calendar year.

For the new year, a new key will be generated and signed by the previous year key, but also by our Master Certification Key:

```
4096R/5C4363F5 2017-06-01 Z-CERT Master Certification Key (used for signing
annual team keys ONLY)
Fingerprint=59A0 7A0E EA4E DD51 9D5B  08A1 F81A E314 5C43 63F5
```

These keys and their signatures can be found at the usual large public key servers, and the current year key also at https://z-cert.nl/pgp/

2.9 Team Members

A list of team members is available at https://z-cert.nl/ons-team/

2.10 Other information

Further information is available on:

- https://z-cert.nl
- https://portal.first.org/directory/Z-CERT
- https://www.trusted-introducer.org/directory/teams/z-cert-nl.html

2.11 Points of Customer Contact

Please contact info@z-cert.nl or +31-33-737-0609 for generic enquiry. Incident-related communications can be sent to cert@z-cert.nl. Constituents and trusted partners are provided with a direct phone number as well. Finally, constituents can reach us via our private chat appliance.

3. Charter

3.1 Mission Statement

Dutch healthcare digitally safe & secure.

Z-CERT supports healthcare providers in preventing and mitigating impact of cybersecurity incidents so that uninterrupted care can be provided and information is secured well.

3.2 Constituency

The constituency of Z-CERT consists of organizations within the healthcare sector in the Netherlands. Many organizations are a member through their umbrella organization. The current constituency consists of approx. 320 organizations.

Healthcare institutions are welcome to join voluntarily but will not be actively approached to join. There currently is no legal requirement for healthcare institutions to join Z-CERT.

Z-CERT functions as an external, sectoral CERT. This means that Z-CERT does not actively monitor the internal network of its members organisations.

3.3 Sponsorship and/or Affiliation

Z-CERT is founded by request of the three largest umbrella organizations in Dutch Healthcare; the NFU, NVZ and Nederlandse GGZ together with the Ministry of Healthcare. Z-CERT works closely with other national and sectoral CERT's within the Netherlands and internationally, and is a member of FIRST, TF-CSIRT, H-ISAC and EH-ISAC.

3.4 Authority

Z-CERT is a foundation with a nonprofit objective. It was founded by several healthcare associations in cooperation with the Dutch Ministery of Healthcare to serve as their joint computer emergency response team. Z-CERT functions in an advisory role and has no authority to make decisions on behalf of its members.

4. Policies

4.1 Types of Incidents and Level of Support

Z-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, within its constituency or in the health care sector at large.

The level of support given by Z-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and Z-CERT's resources at the time. Types of incidents will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, the organisations CERT, or department head for assistance. Z-CERT will support the latter.

While Z-CERT recognizes that variations in the level of system administrator expertise exists, and while Z-CERT will strive to present information and assistance at a level appropriate to each person, Z-CERT will not train system administrators on the fly, and it will not perform system maintenance on their behalf. In most cases, Z-CERT will provide pointers to the information needed to implement appropriate measures.

Z-CERT is committed to keeping its constituents' system administration community informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

Z-CERT has an agreement with its members on how to disseminate information. While there are legal and ethical restrictions on the flow of information, Z-CERT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, Z-CERT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

4.3 Communication and Authentication

In view of the types of information that Z-CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission. Z-CERT also provides a portal that can be used by members to securely communicate with and transfer files to Z-CERT.

Where it is necessary to establish trust, for example before relying on information given to Z-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

In case a healthcare institution has been affected by an ICT security incident, Z-CERT will offer advice on the approach and best resolution method of the incident. Additionally, Z-CERT can conduct limited forensic research into the Modus Operandi, in order to minimize technical and financial damage as well as any reputation risk.

5.1 Incident Response

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred
- Determining the extent of the incident

5.1.2 Incident Coordination

- Facilitating contact with other involved parties
- Providing support for communication with stakeholders and media

5.1.3 Incident Resolution

- Providing advice to the constituent to assist in remediating the vulnerabilities that caused the incident and securing the systems from the effects of the incident
- Providing advice on mitigating actions required to limit the adverse effects of the incident
- Providing any other support requested by the constituent within reasonable and legal limits

5.2 Proactive Activities

Z-CERT checks multiple sources (viruses, worms, botnets, etc.) daily against participants' IP addresses and domain names. Z-CERT will immediately inform the participant(s) and offer advice if a match is detected. Z-CERT provides threat intelligence from trusted sources and constituents automatically to its constituents.

Z-CERT will inform its participants of any vulnerabilities detected in devices, networks and applications, specifically in medical devices, medical networks and medical applications. To those participants affected by a vulnerability, Z-CERT will provide advice on how to best deal with the situation. Z-CERT will also be sending out alerts regarding -threats and current attacks.

Z-CERT shares its knowledge with its participants, facilitates communication channels and meetings for its participants, and hosts network events and theme sessions.

Any vulnerabilities detected in healthcare facility systems, in medical networks and in medical devices by third parties, can be reported to responsibledisclosure@z-cert.nl. Upon receipt of such report, Z-CERT will coordinate the resolution of the vulnerability.

Finally, Z-CERT is always working on new ways to proactively work towards a more secure healthcare sector in the Netherlands and always has multiple projects running to support our mission statement.

6. Incident Reporting Forms

There are no special forms required to report an incident.

7. Disclaimers

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