

CSIRT Description for Z-CERT

Formatted according to RFC2350

1. About this document

1.1 Date of Last Update

This is version 3.0, published September 2026.

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing list.

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:

<https://z-cert.nl/RFC2350-z-cert>

2. Contact Information

2.1 Name of the Team

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

2.2 Address

Stichting 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

Incident alarm number (24/7): +31-85-070-8444
General number: +31-33-737-0609

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

General inquiries: info@z-cert.nl

Incidents and other operational inquiries: cert@z-cert.nl

2.8 Public Keys and Other Encryption Information

Z-CERT uses PGP for encrypted communication.

A PGP key is provided which is changed every calendar year.

For the new year, a new key will be generated and signed by the previous year key and by our Master Certification Key, which holds the following fingerprint:

59A0 7A0E EA4E DD51 9D5B 08A1 F81A E314 5C43 63F5

The current year key is published at: <https://z-cert.nl/pgp/>

2.9 Team Members

A full list of team members is not publicly available. The team members identify themselves to the reporting party with their full name in official communication regarding an incident.

2.10 Other information

Further information is available on:

- <https://z-cert.nl/en>
- <https://www.first.org/members/teams/z-cert>
- <https://www.trusted-introducer.org/trusted-introducer/directory/teams/z-cert-nl/>

2.11 Points of Customer Contact

Please contact info@z-cert.nl or +31-33-737-0609 for generic enquiries.

For incidents, Z-CERT can be contacted via +31-85-070-8444 (24/7) and cert@z-cert.nl.

3. Charter

3.1 Mission Statement

Make Dutch healthcare digitally secure.

Z-CERT supports healthcare organisations 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 is made up of healthcare organisations that are considered essential or important under the 'Cyberbeveiligingswet' (NIS2 directive). Non CBW-entities may report incidents voluntarily but are not subject to mandatory obligations and are generally not entitled to the same level of assistance.

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 is appointed as sectoral CSIRT and partly sponsored by 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 Ministry 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 or issue penalties. For healthcare organizations subjected to the Dutch implementation of the NIS2, Z-CERT performs its duties under this law. Z-CERT is not a regulatory or supervisory authority but is empowered to publicly communicate about an incident that occurs at a constituent when deemed critically necessary.

4. Policies

4.1 Types of Incidents and Level of Support

Z-CERT addresses all types of cybersecurity incidents, which occur, or threaten to occur, in its constituency (see 3.2) or in the healthcare sector at large. The level of support given by Z-CERT varies depending on the type, severity, and impact of the incident; the type of organization; and the available expertise within the organization.

Note that no direct support will be given to end users – they are expected to contact their system administrator, network administrator, the organisation's 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 (technical) 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 references to the information needed to implement appropriate measures.

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

4.2 Cooperation, Interaction and Disclosure of 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 where necessary, Z-CERT will share relevant information when this will assist others in resolving or preventing security incidents.

Z-CERT collaborates both nationally and internationally with relevant parties. This collaboration takes place through various ISACs, the EU CSIRT Network, FIRST, and other relevant forums and organizations. When needed or helpful, Z-CERT also collaborates with law enforcement agencies, vendors, research organizations and hacker communities.

Collaboration and co-operation requests are assessed on a case-by-case basis, based on various internal parameters, including ethical, legal, operational and commercial considerations.

4.3 Communication and Authentication

In view of the types of information that Z-CERT deals with, telephones are considered sufficiently secure to be used even when unencrypted. Unencrypted e-mail is not considered secure, but is sufficient for the transmission of low-sensitivity data. When it is necessary to send highly sensitive

data by e-mail, secure messaging/e-mail platforms or PGP will be used. Network file transfers are considered similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

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 are ascertained and verified to a reasonable degree of trust. Otherwise, relevant and valid information sources are used, such as but not limited to a search of FIRST members, the use of WHOIS and other Internet registration information, along with official or established contact information to ensure that the party is not an impostor. Incoming sensitive e-mails are checked with the originator personally through a secondary contact method or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response – individual organisation

In case a singular healthcare institution has been affected by a particular cybersecurity incident, Z-CERT can perform the following activities for the institution.

5.1.1 Registration

- support in determining whether the threshold value is met
- support in reporting the cybersecurity incident in the NCSC reporting portal

5.1.2 Investigation

- analysis to determine the nature and origin of the incident (identification)
- analysis of suspicious files, such as phishing and malware
- interpret and/or review interim research results received by the affected organization or relevant involved 3rd party

5.1.3 Advise on

- setting up crisis/incident management structure
- stopping the attack (containment)
- removing traces of the attacker(s) (eradication)
- restoring the IT environment (recovery)
- additional security measures in relation to the cybersecurity incident
- providing support when reporting to law enforcement agencies and authorities.

5.1.4 Reporting

- review of investigation/incident reporting (victim organization / third party)
- summarize on work carried out and results

5.1.5 Evaluation

- identify improvements in the handling of the cybersecurity incident
- participate in the organization's incident evaluation

5.2 Incident Response – Sector

The following activities are performed in relation to the healthcare sector as a whole:

- collecting and analyzing incident information and data, such as Indicators of Compromise
- sharing incident information and data
- suggesting courses of action

- coordinating cybersecurity incidents that affect multiple organizations in the sector
- evaluating cybersecurity incidents that affect multiple organizations in the sector
- sharing "lessons learned" from cybersecurity incidents that affect multiple organizations in the sector

5.3 Proactive Activities

Z-CERT provides threat intelligence from trusted sources and constituents automatically to its constituents. Z-CERT monitors multiple sources continuously against organizations' IP addresses and domain names and immediately informs the organization(s) to offer advice if a match is detected.

Z-CERT informs healthcare organizations of any vulnerabilities detected in devices, networks and applications, specifically in medical devices, medical networks and medical applications. To those organizations affected by a vulnerability, Z-CERT provides advice on how to best deal with the situation. Z-CERT additionally sends alerts regarding threats and current attacks.

Z-CERT monitors entities' external assets for vulnerable or misconfigured systems and sends automatic reports on any findings.

Z-CERT shares its knowledge with healthcare organizations, facilitates communication channels and meetings for healthcare organizations, 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 cvd@z-cert.nl. Upon receipt of such report, Z-CERT will coordinate the resolution of the vulnerability.

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

6. Incident Reporting Forms

Incidents can be reported through the Z-CERT web portal – <https://mijn.z-cert.nl>. Significant incidents, as defined by the Dutch implementation of the NIS2, must be reported in the national reporting system hosted by the National Cyber Security Center – <https://mijn.ncsc.nl>.

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.