Responsible Disclosure

Responsible Disclosure Nederlands

Stichting Laurens hecht veel belang aan de veiligheid van haar (medische) apparatuur, programmatuur en diensten. Ondanks de zorg voor de beveiliging hiervan kan het voorkomen dat er toch sprake is van een kwetsbaarheid. Als u zo'n kwetsbaarheid ontdekt, kunt u dit veilig aan ons melden (via onze partner Z-CERT). Deze aanpak is de zogenaamde Coordinated Vulnerability Disclosure. Op deze manier kan Laurens samen met Z-CERT beschermende maatregelen treffen.Als u een kwetsbaarheid heeft gevonden horen wij dit graag, zodat we zo snel als mogelijk maatregelen kunnen treffen. Hierin werken wij samen met Z-CERT.

English? Click here to send CVD-notifications

Melding van een kwetsbaarheid

Als u een kwetsbaarheid heeft gevonden horen wij dit graag, zodat we zo snel als mogelijk maatregelen kunnen treffen. Hierin werken wij samen met Z-CERT.

Wanneer u via ons Coordinated Vulnerability Disclosure-beleid kwetsbaarheden aan ons meldt, dan hebben wij geen reden om juridische consequenties te verbinden aan uw melding, indien u zich houdt aan de volgende regels:

- Verzeker u ervan dat uw melding 'in scope' is. Onderaan deze pagina kunt u controleren wat als niet 'in scope' wordt beschouwd.

- U meldt uw bevindingen door gebruik te maken van het volgende mailtemplate. Stuur dit volledig ingevuld naar Z-CERT, eventueel gebruik makend van Z-CERT's publieke PGP-sleutel.

- In uw melding geeft u voldoende informatie, zodat het probleem te reproduceren is. Op die manier kunnen wij het zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden is soms meer informatie gewenst/noodzakelijk. U kunt een proof of concept meesturen.

- U misbruikt de geconstateerde kwetsbaarheid niet door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door gegevens van derden in te zien, te verwijderen of aan te passen.

- Als u vermoedt dat u via een kwetsbaarheid medische gegevens kan inzien, vragen wij u dit niet zelf te verifiëren maar dit door ons te laten doen.

- U deelt uw bevindingen niet met anderen, voordat het is opgelost. Daarnaast vragen we u om alle vertrouwelijke gegevens die u heeft verkregen, na het dichten van het lek, direct te wissen.

- U doet geen aanval(len) op onze fysieke beveiliging en maakt geen gebruik van social engineering, (distributed) denial of service, spam, brute-force aanvallen en/of applicaties van derden.

Hoe wij omgaan met uw melding

- Z-CERT behandelt uw melding vertrouwelijk en deelt uw persoonlijke gegevens niet met derden zonder uw toestemming, tenzij dit wettelijk verplicht is.

- U krijgt een ontvangstbevestiging van Z-CERT en binnen 5 werkdagen ontvangt u een reactie op uw melding met een beoordeling van de melding en een verwachte datum voor een oplossing.

- Als melder van het probleem houdt Z-CERT u op de hoogte van de voortgang van het oplossen van het probleem.

- In berichtgeving over het gemelde probleem zal Z-CERT, als u dit wenst, uw naam vermelden als de ontdekker.

- Als dank voor uw hulp biedt Z-CERT een beloning aan. Die beloning kan variëren afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding.

We streven ernaar om alle problemen zo snel mogelijk op te lossen. Samen overleggen we daarna over de meerwaarde van een eventuele publicatie van het opgeloste probleem.

Niet in scope

Z-CERT neemt geen triviale kwetsbaarheden of security-issues die niet misbruikt kunnen worden, in behandeling. Hieronder staan voorbeelden van bekende kwetsbaarheden en security-issues die buiten bovenstaande regeling vallen. Dit houdt niet in dat ze niet opgelost zouden moeten worden, echter bij ons CVD-proces gaat het om het melden van zaken waar direct misbruik van gemaakt kan worden. Bijvoorbeeld een kwetsbaarheid waar een werkende exploit voor bestaat of een misconfiguratie waardoor een bestaande security control te omzeilen is. Deze lijst is afgeleid van de lijst die het CERT van SURF hanteert.

1. HTTP 404 codes/pages or other HTTP non-200 codes/pages and content spoofing/text injections in these pages
2. Fingerprinting/version disclosures op public services
3. Public files or directories that do not contain confidential information
4. All disclosures of confidential/sensitive information will be judged by Z-CERT or the healthcare organization involved, and might be labeled “out of scope” if they do not pose a significant risk.
5. Click jacking, problems that can only be exploited by clickjacking
6. No secure/HTTP-only flags on unconfidential cookies
7. OPTIONS HTTP method enabled
8. Rate-limiting without clear impact
9. All issues related to HTTP security headers, for example:
    1. X-Frame-Options
    2. X-XSS-Protection
    3. X-Content-Type-Options
    4. Content-Security-Policy
    5. Strict-Transport-Security
10. SSL security configuration issues, for example:
    1. SSL Forward secrecy disabled

11. No TXT record for DMARC or a missing CAA-record
12. Host header injection
13. Reports of outdated versions of any software without a proof of concept of a working exploit
14. Absence of security best practices or hardening measures. Though important, they are not within scope of a CVD process. Example:
    1. xmlrpc.php/wp-json of a wordpress website
    2. Absence of rate limiting measures.
15. Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
16. Social engineering of healthcare organisation staff or contractors. For example creating phishing pages.
17. Issues that result in Denial of Service (DoS) to organisations servers at the network or application layer.
18. Issues that require unlikely user interaction
19. Cross-site Request Forgery with minimal security impact
20. Issues related to software or protocols not under the organizations control. For example known issues with ARP or HL7.
21. It is possible that your report on an issue overlaps with a report on the same issue by another individual. In this case we will only accept the first report received by us.

Mailtemplate

Aan	cvd@z-cert.nl
Cc	
Bcc	
Onderwerp	CVD-melding

Beste Z-CERT,

Hierbij wil ik de volgende kwetsbaarheid melden.

Mijn naam is [je naam]. Ik heb een [type kwetsbaarheid] kwetsbaarheid gevonden bij [naam van de organisatie van het systeem].

Ik verklaar dat mijn onderzoek in lijn is met het CVD-beleid van Z-CERT en heb gecontroleerd of de melding in scope is volgens www.z-cert.nl/cvd-melden/.

Het kwetsbare systeem is: [IP-adres/domein/url]

Omschrijving: [Leg de kwetsbaarheid stap voor stap uit en voeg een werkende proof of concept toe. Indien je de proof of concept als bijlage wilt meesturen, gebruik dan een standaard bestandsformaat.

Impact: [Leg uit wat de impact van de kwetsbaarheid is.]

Oplossing: [Leg uit hoe de kwetsbaarheid te mitigeren is.]

[Als je jouw melding versleuteld wilt versturen, stuur dan je publieke pgp-sleutel mee als bijlage.]

Met vriendelijke groet,

[jouw naam]

Responsible Disclosure English

At Laurens we find the safety of our own systems very important. Despite our concern for the security of our systems, it is possible that there is a weak spot. If you have found a vulnerability, please let us know so that we can take measures as quickly as possible. We work together with Z-CERT on this.

Reporting a vulnerability

If you have found a weak spot in one of our systems, we would like to hear this so that we can take measures (together with our partner Z-CERT) as soon as possible. We would like to work with you to better protect our participants and our systems. If you comply with our Coordinated Vulnerability Disclosure policy we have no reason to take legal action against you regarding the reported vulnerability.

We ask you to:

- Make sure that your findings are in scope. Further on this page you can check what is considered to be out-of-scope.
- Please use this CVD-form to send your findings to Z-CERT, encrypted with our PGP-key.
- Provide adequate information to allow us to investigate and reproduce the vulnerability. Fill out every aspect of the CVD-form. This helps to resolve the problem as quickly as possible. An IP address or URL of the affected system with a description of the vulnerability will usually be sufficient, although more information might be necessary for more complex vulnerabilities. You may add a proof of concept.
- Do not exploit vulnerabilities, e.g. by downloading more data than is needed to demonstrate the vulnerability, looking into third-party data, deleting or modifying data.
- If you suspect to have access to medical data we ask you to let us verify this.
- Do not share information on vulnerabilities until they have been resolved and erase any obtained data as soon as the problem is solved.
- Do not attack (physical) security using social engineering, distributed denial of service, spam, brute force attacks, third-party applications for instance, or other types of attacks.

How we will handle your report

- Z-CERT will treat your report confidentially and will not share your personal data unless required by law.
- Z-CERT will send you a confirmation of receipt and will respond within five working days with an evaluation of your report and an expected resolution date.
- Z-CERT will keep you informed of the progress in resolving the problem.
- In communication about the reported problem we will mention your name as the discoverer of the problem (unless you desire otherwise).
- Z-CERT offers a thank you reward which can vary depending on the severity of the vulnerability and the quality of the report.

We strive to resolve any vulnerability as soon as possible. Once the problem has been resolved we will decide in consultation whether and how details will be published.

Not in scope

Z-CERT will not process reports of vulnerabilities or security issues that can not be abused or are trivial. Below are a couple of examples of known vulnerabilities and issues that are outside the scope. This does not mean they are not important or should not be resolved, however our CVD process is meant for issues that can be actively abused. For example, vulnerabilities that can be abused by a public available exploit or a misconfiguration that can be used to bypass an existing security control. This list of exclusions is derived from a list used by the CERT of Surf.

1. HTTP 404 codes/pages or other HTTP non-200 codes/pages and content spoofing/text injections in these pages
2. Fingerprinting/version disclosures op public services
3. Public files or directories that do not contain confidential information
4. All disclosures of confidential/sensitive information will be judged by Z-CERT or the healthcare organization involved, and might be labeled “out of scope” if they do not pose a significant risk.
5. Click jacking, problems that can only be exploited by clickjacking
6. No secure/HTTP-only flags on unconfidential cookies
7. OPTIONS HTTP method enabled
8. Rate-limiting without clear impact
9. All issues related to HTTP security headers, for example:
    1. X-Frame-Options
    2. X-XSS-Protection
    3. X-Content-Type-Options
    4. Content-Security-Policy
    5. Strict-Transport-Security
10. SSL security configurattion issues, for example:
    1. SSL Forward secrecy disabled

11. No TXT record for DMARC or a missing CAA-record
12. Host header injection
13. Reports of outdated versions of any software without a proof of concept of a working exploit
14. Absence of security best practices or hardening measures. Though important, they are not within scope of a CVD process. Example:
    1. xmlrpc.php/wp-json of a wordpress website
    2. Absence of rate limiting measures.
15. Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
16. Social engineering of healthcare organisation staff or contractors. For example creating phishing pages.
17. Issues that result in Denial of Service (DoS) to organisations servers at the network or application layer.
18. Issues that require unlikely user interaction
19. Cross-site Request Forgery with minimal security impact
20. Issues related to software or protocols not under the organizations control. For example known issues with ARP or HL7.
21. It is possible that your report on an issue overlaps with a report on the same issue by another individual. In this case we will only accept the first report received by us.

Mailtemplate

To	cvd@z-cert.nl
Cc	
Bcc	
Subject	CVD-report

To Z-CERT,

I would like to report the following vulnerability.

My name is [your name]. I have found a [vulnerability type] vulnerability at [system organization name].

I declare that my investigation is in line with Z-CERT's CVD policy and have checked whether the report is in scope according to www.z-cert.nl/cvd-melden/.

The vulnerable system is: [IP address/domain/url]

Description: [Explain the vulnerability step by step and include a working proof of concept. If you want to send the proof of concept as an attachment, please use a standard file format.

Impact: [Explain the impact of the vulnerability.]

Solution: [Explain how to mitigate the vulnerability.]

[If you want to send your notification encrypted, please send your public PGP key as an attachment.]

Yours sincerely,

[your name]