Coordinated Vulnerability Disclosure

Amphia 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.

Melding maken van een kwetsbaarheid
Als u zo'n kwetsbaarheid ontdekt, kunt u dit veilig aan ons melden. Deze aanpak is de zogenaamde Coordinated Vulnerability Disclosure. Amphia wil graag met u samenwerken om onze klanten en systemen nog beter te kunnen beschermen.

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.
Stichting Z-CERT is de organisatie die voor Amphia Coordinated Vulnerability Disclosure meldingen afhandelt. Zij werken samen met u als melder en met Amphia om te zorgen dat uw melding wordt opgepakt. Wij vragen u zich te houden aan de volgende regels:

- U meldt uw bevindingen bij Stichting Z-CERT door een e-mail te sturen naar cvd@z-cert.nl en gebruikt hierbij Z-CERT's publieke PGP sleutel. Zie Kwetsbaarheid melden - Z-CERT
- 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.
- Ons Coordinated Vulnerability Disclosure beleid is geen uitnodiging om ons bedrijfsnetwerk (onze systemen) uitgebreid actief te scannen op kwetsbaarheden.

Hoe wij omgaan met uw melding
- Amphia en Z-CERT behandelen uw melding vertrouwelijk en delen 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 uw melding overlap vertoont met een eerdere melding, dan wordt alleen de eerste in behandeling genomen.

Niet in scope
Z-CERT neemt meldingen niet in behandeling als het gaat om triviale kwetsbaarheden of security-issues die niet misbruikt kunnen worden.

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 beheersmaatregel 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 on 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.

- English -

Coordinated Vulnerability Disclosure

At Amphia we work hard to maintain and improve the security of our (medical) devices, systems and services. No matter how much effort we put into system security, there might be vulnerabilities present.

Reporting a vulnerability
If you discover a vulnerability you can report it safely via our Coordinated Vulnerability Disclosure. This way Amphia can take safety measures to protect its clients and systems better.

If you comply with our Coordinated Vulnerability Disclosure policy we have no reason to take legal action against you regarding the reported vulnerability.
Stichting Z-CERT is the organization that handles Coordinated Vulnerability Disclosure reports on behalf of Amphia. They work together with you as the reporter and with Amphia to ensure that your report is properly addressed. We ask that you adhere to the following rules:

- Report your findings to Z-CERT by sending an e-mail to cvd@z-cert.nl. Encrypt it using Z-CERT's PGP key. See Coordinated Vulnerability Disclosure - Z-CERT
- Provide adequate information to allow us to investigate and reproduce the vulnerability. 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 that you may 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.
- Our Coordinated Vulnerability Disclosure policy is not an invitation to extensively or actively scan our corporate network (our systems) for vulnerabilities.

How we will handle your report
- Amphia and Z-CERT will treat your report confidentially and will not share your personal data unless required by law.
- You will receive a confirmation of receipt and we 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).
- If your report overlaps with a report on the same issue by another individual we will only accept the first report received by us.

Not in scope

Z-CERT does not process reports concerning trivial vulnerabilities or security issues that cannot be exploited. Below are examples of known vulnerabilities and security issues that are out of scope of the above policy. This does not mean they should not be resolved; however, within our CVD process we focus on reporting issues that can be directly exploited.

For example, a vulnerability for which a working exploit exists, or a misconfiguration that allows an existing security measure to be bypassed.

This list is based on the list used by SURF's CERT.

1. HTTP 404 codes/pages or other HTTP non-200 codes/pages and content spoofing/text injections in these pages
2. Fingerprinting/version disclosures on 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.