Coordinated Vulnerability Disclosure (CVD)

Het Canisius Wilhelmina Ziekenhuis (CWZ) 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. Deze aanpak is de zogenaamde *Coordinated Vulnerability Disclosure*. Op deze manier kan CWZ beschermende maatregelen treffen.

Melding maken van een kwetsbaarheid
Als u een kwetsbaarheid heeft gevonden horen wij dit graag, zodat we zo snel als mogelijk maatregelen kunnen treffen. CWZ wil graag met u samenwerken om onze klanten en systemen nog beter te kunnen beschermen.

Ons Coordinated Vulnerability Disclosure beleid is geen uitnodiging om ons bedrijfsnetwerk (onze systemen) uitgebreid actief te scannen op kwetsbaarheden. Wij monitoren ons netwerk, hierdoor is de kans groot dat een scan wordt opgemerkt door onze IT-afdeling en is er kans dat zij hier onderzoek naar gaan doen en er mogelijk onnodige kosten worden gemaakt.

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. 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. U kunt daarbij gebruik maken van de PGP-sleutel. Stichting Z-CERT is de organisatie die voor CWZ Coordinated Vulnerability Disclosure meldingen afhandelt. Zij werken samen met u als melder en met CWZ om te zorgen dat uw melding wordt opgepakt.
- 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 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

- CWZ 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 CWZ, als u dit wenst, uw naam vermelden als de ontdekker.
- Als dank voor uw hulp biedt CWZ een beloning aan. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een T-shirt tot cadeaubonnen voor maximaal 300 euro.

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.

Publicatiedatum: april 2021.

Niet in scope (informatie Z-CERT)

Z-CERT neemt geen triviale kwetsbaarheden of securityissues die niet misbruikt kunnen worden, in behandeling. Hieronder staan voorbeelden van bekende kwetsbaarheden en securityissues die buiten bovenstaande regeling vallen. Dit houdt niet dat ze niet opgelost zouden moeten worden, echter bij ons CVD-proces gaat het om 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 securitycontrol te omzeilen is. Deze lijst is afgeleid van de lijst van die het CERT van Surf hanteert (https://www.surf.nl/responsible-disclosure-surf).

– HTTP 404 codes/pagina's of andere HTTP non-200 codes/pagina's en content spoofing/text injecting op deze pagina's
– Fingerprinting/versievermelding op publieke services
– Publieke bestanden of directories met ongevoelige informatie (bijvoorbeeld robots.txt)
– Clickjacking en problemen die alleen te exploiten zijn via clickjacking
– Geen secure/HTTP-only flags op ongevoelige cookies
– OPTIONS HTTP method ingeschakeld
– Rate limiting kwetsbaarheden zonder duidelijke impact

Alles gerelateerd tot HTTP security headers, bijvoorbeeld:
– Strict-Transport-Security
– X-Frame-Options
– X-XSS-Protection
– X-Content-Type-Options
– Content-Security-Policy

– Issues met SSL-configuratie
– SSL Forward secrecy uitgeschakeld

– Ontbrekende TXT record voor DMARC of CAA record
– Host header injection
– Rapporteren van verouderde versies van enige software zonder een proof of concept van een werkende exploit