# Beleid Responsible Disclosure

Auteur: Surplus
Datum: 15 augustus 2023
Versie: 0.1
Status: Definitief

# Beleid Responsible Disclosure

Bij Surplus vinden wij de veiligheid van onze systemen, programmatuur en diensten erg belangrijk. Ondanks onze zorg voor de beveiliging hiervan kan het voorkomen dat er toch een kwetsbaarheid is. 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 Surplus beschermende maatregelen treffen, want we willen graag met u samenwerken om onze gebruikers, onze systemen en de gegevens van onze patiënten en medewerkers nog beter beschermen.

Ons beleid voor responsible disclosure is **geen** uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren namelijk ons bedrijfsnetwerk. Dit maakt de kans groot dat een scan wordt opgemerkt door ons Computer Emergency Response Team (CERT) of IT-afdeling, mogelijk leidend tot een onderzoek en het maken van onnodige kosten. Computervredebreuk is in beginsel strafbaar, ook bij ethisch hacken. Echter, als u zich aan de onderstaande regels houdt, hebben wij geen reden om juridische stappen te verbinden aan uw melding. Het Openbaar Ministerie behoudt echter altijd het recht zelf te beslissen of u strafrechtelijk vervolgd wordt. Het Openbaar Ministerie heeft hierover een beleidsbrief gepubliceerd.

## Wij vragen u:

- De bevinding(en) te melden bij de 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 Surplus de Coordinated Vulnerability Disclosure meldingen afhandelt. Zij werken samen met u als melder en met Surplus om te zorgen dat uw melding wordt opgepakt.
- In uw melding voldoende informatie te geven, 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.
- De geconstateerde kwetsbaarheid niet te misbruiken. 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.

- Geen bevindingen te delen 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.
- Geen aanval(len) te doen op onze fysieke beveiliging en geen gebruik te maken van social engineering, distributed denial of service, spam, brute-force aanvallen en/of applicaties van derden.

## Wij beloven u:

- Surplus 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 Surplus, als u dit wenst, uw naam vermelden als de ontdekker.

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 securityissues die niet misbruikt kunnen worden, in behandeling. Hieronder staan voorbeelden van bekende kwetsbaarheden en securityissues die buiten bovenstaande regeling vallen. Dit betekent 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 die Z-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