Laatste gewijzigd: Juni 2023

Beveiliging niet in orde? Meld het ons.

Responsible Disclosure

Bij Franciscus Gasthuis & Vlietland (hierna: Franciscus) vinden wij de veiligheid van onze digitale omgeving en informatiesystemen erg belangrijk. Patiënten, bezoekers en medewerkers mogen van Franciscus verwachten dat hun gegevens bij ons veilig zijn. Ondanks onze zorg voor de beveiliging van onze systemen kan het onverhoopt voorkomen dat er toch een zwakke plek aanwezig is of ontstaat die nog niet ontdekt is.
Wanneer u een zwakke plek/kwetsbaarheid in de ICT-systemen of het IT netwerk van Franciscus constateert, horen wij dit graag van u, zodat wij zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze patiëntgegevens, medewerkersgegevens en onze systemen te beschermen.

Hoe kan ik een zwakke plek in de ICT beveiliging van Franciscus melden?

Franciscus vraagt u om uw bevindingen zo snel mogelijk na ontdekking te melden aan het IT Security team van Franciscus via itsecurity@franciscus.nl.

- Meld de kwetsbaarheid alléén aan Franciscus en niet aan de buitenwereld. Dit heet Responsible Disclosure.

Waar moet u aan denken bij Responsible Disclosure?

Wanneer u een melding doet van een kwetsbaarheid denk dan aan de volgende zaken:

- Geef voldoende informatie om het probleem te kunnen reproduceren.
  Zo kan Franciscus gericht onderzoek en het probleem zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij ingewikkeldere kwetsbaarheden kan meer informatie nodig zijn.
- Laat uw contactgegevens (e-mailadres of telefoonnummer) achter zodat Franciscus contact met u kan opnemen.
- Doe de melding zo snel mogelijk na ontdekking van de kwetsbaarheid.
- Deel de informatie over het beveiligingsprobleem niet met anderen, totdat het probleem is opgelost.
- Ga verantwoordelijk om met de kennis over het beveiligingsprobleem.
  Verricht geen *(strafbare)* handelingen die verder gaan dan datgene wat nodig is om het beveiligingsprobleem aan te tonen. Stafbare handelingen kunnen leiden tot vervolging en/of een schadeclaim.

Responsible Disclosure is géén uitnodiging tot actief scannen

Het beleid voor responsible disclosure is geen uitnodiging om onze ICT-systemen actief te scannen om zwakke plekken te ontdekken. Franciscus monitort zelf haar ICT-systemen en doet er alles aan om kwetsbaarheden te verhelpen.

Laatste gewijzigd: Juni 2023

Wat mag u van Franciscus verwachten?

Heeft u een melding gedaan van een zwakke plek in de beveiliging van Franciscus en wordt daarbij voldaan aan de hieronder genoemde voorwaarden, dan behandeld Franciscus uw melding als volgt:

- Franciscus behandelt uw melding strikt vertrouwelijk en deelt uw persoonlijke gegevens niet met derden zonder uw expliciete toestemming, tenzij dit wettelijk of door een rechterlijke uitspraak verplicht wordt gesteld.
- Franciscus reageert binnen 1 werkweek op uw melding. Deze reactie bevat een beoordeling van de melding en een verwachte datum voor een oplossing.
- Franciscus houdt u als melder op de hoogte van de voortgang van het oplossen van het probleem.
- Franciscus zal samen met u bepalen of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker.
- Als dank voor uw hulp biedt Franciscus u een ludieke beloning *(een goodiebag o.i.d.)* voor elke melding van een nog onbekend en serieus beveiligingsprobleem bij Franciscus. Deze beloning zal nooit in geldelijke vorm zijn. *(zie ook de voorwaarden: C. Niet in scope)*
- De situatie kan zich voordoen dat de door u gemelde kwetsbaarheid reeds eerder bij ons is gemeld door een andere melder. In dit geval zullen wij alléén de melding accepteren die als eerste bij ons is binnengekomen.

Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem, nadat het is opgelost.

Reageert Franciscus niet of niet goed op uw melding?

Indien u binnen de genoemde termijnen geen reactie krijgt van Franciscus kunt u het landelijke Zorg-CERT op de hoogte brengen via cert@z-cert.nl. Zij vervullen dan de rol van intermediair en zullen het ziekenhuis hierover benaderen. Verdere gegevens vind u op Contact - Z-CERT

VOORWAARDEN

A. Maak géén misbruik van de kwetsbaarheid!

Het misbruiken van kwetsbaarheden is illegaal en dus strafbaar. Als u een kwetsbaarheid ontdekt, maak hier dan geen misbruik van door bijvoorbeeld:

- meer data te downloaden dan noodzakelijk is om het lek aan te tonen,
- door onnodig gegevens in te zien, aan te passen, toe te voegen dan wel te verwijderen;
- malware te plaatsen;
- gegevens in een systeem te kopiëren (een alternatief hiervoor is een directorylisting of een screenshot maken van een systeem);
- veranderingen aan te brengen in systemen en of data van Franciscus;
- herhaaldelijk toegang te verkrijgen tot het systeem *(vaker en langer dan noodzakelijk om de kwetsbaarheid aan te tonen)*;

- toegang te delen met anderen;
- de kwetsbaarheid openbaar te maken voor anderen;
- gebruik te maken van het zogeheten ‘brute forcen’ van toegang tot systemen;
- gebruik te maken van denial-of-service aanvallen of social engineering.
- Het gebruik van geautomatiseerde scantools en het versturen van niet-geverifieerde output van dergelijke tools. Scantools genereren vaak ‘false positives’. Alleen door de melder geverifieerde beveiligingsfouten worden door Franciscus in behandeling genomen

B. Strafrechtelijke vervolging

Het is mogelijk dat u tijdens uw onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Voldoet u bij uw melding aan bovenstaande voorwaarden, dan onderneemt Franciscus geen juridische stappen tegen u, maar zijn wij juist blij met uw hulp.

Het Openbaar Ministerie heeft echter altijd het recht om over te gaan tot strafrechtelijke vervolging. Hierover heeft het Openbaar Ministerie deze beleidsbrief gepubliceerd.

C. Niet in scope

Franciscus geeft **geen beloning** voor triviale kwetsbaarheden óf bugs die niet misbruikt kunnen worden. Hierbij kunt u denken aan de volgende voorbeelden die buiten bovenstaande regeling vallen:

1. HTTP 404 codes/pagina’s of andere HTTP non-200 codes/pagina’s en content spoofing/text injecting op deze pagina's,
2. fingerprinting/versievermelding op publieke services
3. ontbrekende best practices of output van geautomatiseerde scanhulpmiddelen zonder bewijs van exploiteerbaarheid;
4. output van geautomatiseerde scans van hulpprogramma's. Bijvoorbeeld: Web-, SSL / TLS-scan, Nmap-scanresultaten, enz.
5. publieke bestanden of directories met ongevoelige informatie (bijvoorbeeld robots.txt),
6. clickjacking en problemen die alleen te exploiten zijn via clickjacking,
7. geen secure/HTTP-only flags op ongevoelige cookies,
8. alles gerelateerd tot HTTP security headers, bijvoorbeeld:
    - Strict-Transport-Security
    - X-Frame-Options
    - X-XSS-Protection
    - X-Content-Type-Options
    - Content-Security-Policy
9. issues met SSL-configuratie, bijvoorbeeld:
    - SSL Forward secrecy uitgeschakeld
    - zwakke/onveilige cipher suites,
10. issues met SPF, DKIM of DMARC, DNSSEC of CAA-records
11. verouderde versies van enige software zonder een proof of concept van een werkende exploit,
12. informatieblootstelling in metadata.

Laatste gewijzigd: Juni 2023