UMC Utrecht

Beleid responsible disclosure

Bij het UMC Utrecht vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag zodat wij zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze gebruikers, onze systemen en de gegevens van onze patiënten en medewerkers beter te kunnen beschermen.

Ons beleid voor responsible disclosure is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren ons bedrijfsnetwerk. Hierdoor is de kans groot dat een scan wordt opgepikt, dat er door ons Computer Emergency Response Team (CERT) onderzoek wordt gedaan en er mogelijk onnodige kosten worden gemaakt.

Computervredebreuk is in beginsel strafbaar, ook bij ethisch hacken. Maar als u zich aan de onderstaande regels heeft gehouden, zullen wij geen juridische stappen tegen u ondernemen betreffende de melding. Het Openbaar Ministerie behoudt altijd het recht zelf te beslissen of u strafrechtelijk vervolgd wordt. Het Openbaar Ministerie heeft hierover een beleidsbrief gepubliceerd.

Bezoekadres:
Heidelberglaan 100
3584 CX Utrecht

Postadres:
Postbus 85500
3508 GA Utrecht

Wij vragen u:

- Uw bevindingen zo snel mogelijk te mailen naar cert@umcutrecht.nl. Versleutel uw bevindingen met onze PGP key (*asc)* om te voorkomen dat de informatie in verkeerde handen valt.
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door het veranderen of verwijderen van gegevens en extra terughoudendheid te betrachten bij persoonsgegevens.
- De kwetsbaarheid niet met anderen te delen totdat het is opgelost.
- Ons voldoende informatie te geven om de kwetsbaarheid te reproduceren zodat wij die zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem, een omschrijving van de kwetsbaarheid en de uitgevoerde handelingen voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Openbaar maken is pas toegestaan als de melder en het UMC Utrecht zijn overeengekomen dat de kwetsbaarheid openbaar gemaakt kan worden, alle betrokken organisaties goed zijn geïnformeerd en het UMC Utrecht heeft aangegeven dat de kwetsbaarheid is opgelost.
- Als een kwetsbaarheid niet of moeilijk op te lossen is, of indien er hoge kosten mee gemoeid zijn, is de melder alleen gerechtigd de kwetsbaarheid openbaar te maken na uitdrukkelijke toestemming van het UMC Utrecht. Het UMC Utrecht wordt graag betrokken bij een eventuele publicatie over de kwetsbaarheid.

Wat wij beloven:

- Wij reageren binnen 5 werkdagen op uw melding met een bevestiging van ontvangst en een eerste inschatting van de legitimiteit en de ernst van de gemelde kwetsbaarheid.
- Wij houden u op de hoogte van de voortgang van het oplossen van de kwetsbaarheid.
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen.
- Anoniem of onder pseudoniem melden is mogelijk. Het is voor u goed om te weten dat dit wel betekent dat wij dan geen contact kunnen opnemen over bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek of eventuele publicatie van de kwetsbaarheid.
- Indien de Information Security Officer besluit om een bredere ICT-community of het algemene publiek te informeren over de kwetsbaarheid, wordt u hiervan op de hoogte gebracht.
- In berichtgeving over de gemelde kwetsbaarheid zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker van de kwetsbaarheid.
- Wij streven er naar om alle problemen zo snel mogelijk op te lossen en alle betrokken partijen op de hoogte te houden.