Facilicom

Coördinated Vulnerability Disclosure (CVD-) Beleid

Facilicom vindt de veiligheid van haar systemen zeer belangrijk. Toch kan het voorkomen dat er een zwakke plek zit in de beveiliging van één van onze systemen. Vind je een zwakke plek, dan vragen wij je, dit direct bij ons te melden. Zo kunnen wij snel maatregelen treffen om de beveiliging van onze systemen te verbeteren en onze informatie beter te beschermen. Wanneer je een melding moet doen en hoe je dit het beste kunt doen lees je in dit Coördinated Vunerability Disclosure (CVD-)beleid.

Wat zijn de uitgangspunten van ons CVD-beleid?

Alle meldingen worden vertrouwelijk behandeld en uiteraard delen wij jouw (persoonlijke) gegevens niet met anderen zonder jouw toestemming. Wij moeten dit alleen doen als wij hier wettelijk toe verplicht zijn. Doe je een melding aan de hand van dit beleid, dan ondernemen wij geen juridische stappen naar aanleiding van je melding.

Nadat je een melding gedaan hebt laten wij je binnen 3 werkdagen weten of wij je melding in goede orde ontvangen hebben. Binnen 5 werkdagen reageren wij op jouw melding met de beoordeling van je melding.

Wij streven er naar om het door jou gemelde beveiligingsprobleem binnen 60 dagen op te lossen. In overleg met jou bepalen we een termijn en bepalen we of, en op welke wijze, we communiceren met de buitenwereld over het door jou gevonden beveiligingsprobleem.

Voor welke kwetsbaarheden kan je een CVD-melding bij ons maken?

Je kan bij ons kwetsbaarheden melden die een risico vormen voor de beveiliging van één van onze systemen. Bijvoorbeeld een kwetsbaarheid die het mogelijk maakt om een login-formulier te omzeilen of waardoor je onbedoeld toegang hebt tot een database met persoonsgegevens.

Hoe maak je een CVD-melding bij ons?

Je kan op twee manieren een melding bij ons maken:

1. Door het Meldformulier in te vullen.
2. Door gebruik te maken van onze beveiligde e-mail omgeving. Klik hier voor meer informatie.

Beschrijf in jouw melding zo duidelijk mogelijk hoe we het probleem kunnen reproduceren. Dit helpt ons bij het vinden van een oplossing. Vergeet vooral niet te vermelden om welk systeem het gaat en welke kwetsbaarheid er volgens jou in het systeem zit.

Is het probleem een opeenvolging van meerdere stappen en/of handelingen? Beschrijf deze dan stap-voor-stap. Het kan zijn dat wij naar aanleiding van jouw melding vragen hebben. Daarom vragen we je een e-mailadres of telefoonnummer achter te laten zodat wij contact kunnen opnemen. Dit is echter niet verplicht.

Kunnen wij het volgende met elkaar afspreken?

- Je meldt de kwetsbaarheid zo snel mogelijk nadat je deze hebt ontdekt.
- Je deelt je bevindingen alleen met ons. Over verdere communicatie maken wij graag afspraken met je.
- Je maakt geen (actief) misbruik van het beveiligingsprobleem door bijvoorbeeld moedwillig schade aan ons systeem aan te richten of informatie te kopiëren.

In ieder geval:

- Plaats je geen malware.
- Kopieer, wijzig of verwijder je geen informatie op ons systeem.
- Breng je geen veranderingen aan in het systeem die niet noodzakelijk zijn voor het aantonen van de kwetsbaarheid.
- Plaats je geen brute-force aanval op een van onze systemen.
- Maak je geen gebruik van denial-of-service en/of social engineering.

Wanneer hoef je geen melding te doen?

Niet elke afwijking in een systeem is een beveiligingsprobleem. Over het algemeen leiden de volgende afwijkingen niet tot een onveilige situatie. Van de onderstaande afwijkingen hoef je dan ook geen melding te maken:

- Een afwijking die geen impact heeft op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie.
- De mogelijkheid tot cross-site scripting op een statische website of op een website waarop geen gevoelige (gebruikers)informatie wordt verwerkt.
- De afwezigheid van HTTP security headers zoals gebruikt door onder andere Cross-Origin Resource Sharing (CORS), tenzij deze afwezigheid aantoonbaar tot een beveiligingsprobleem leidt.

Wanneer je er niet zeker van bent of de door jouw gevonden afwijking gemeld moet worden, neem dan contact met ons op. Dit kan door middel van een e-mail te sturen naar informatiebeveiliging@facilicom.nl. Wij bespreken dan samen of er sprake is van een beveiligingsprobleem en of deze gemeld moet worden of niet.

Heb je vragen?

Voor vragen en opmerkingen die **niet** gerelateerd zijn aan Coördinated Vulnerability Disclosure, maar **wel** gerelateerd zijn aan cybersecurity, kan je contact opnemen met ons Security Office via informatiebeveiliging@facilicom.nl.