

Responsible Disclosure

Bij het Udens College 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, horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar cert@udenscollege.nl. Versleutel uw bevindingen met onze PGP key* om te voorkomen dat de informatie in verkeerde handen valt;
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, verwijderen of aanpassen;
- Het probleem alleen aan het Udens College te melden en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen;
- Geen gebruik te maken van aanvallen waarbij de systemen schade of uitval kunnen ondervinden;
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 1 werkdag op uw melding;
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding;
- 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. Melden onder een pseudoniem is mogelijk;
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker;
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding. Hierbij kan bijvoorbeeld gedacht worden aan een taart ter compensatie;
- Wij streven er naar om alle problemen zo snel mogelijk op te lossen.

Meer informatie over informatiebeveiling staat in ons protocol informatiebeveiligingsincidenten en datalekken.

* de PGP key is te bereiken via: <https://www.udenscollege.nl/cert-pgp-key.zip>