CONCLUSION

Responsible Disclosure Conclusion

Bij Conclusion vinden wij de veiligheid van onze systemen zeer belangrijk. Ondanks onze zorg voor de veiligheid van onze systemen kan het voorkomen dat er toch onbedoelde kwetsbaarheden aanwezig zijn.

Als u een kwetsbaarheid in één van onze systemen heeft ontdekt, stellen wij het bijzonder op prijs wanneer u deze kwetsbaarheid zo snel als mogelijk meldt, zodat wij noodzakelijke maatregelen kunnen treffen. Wij werken graag met u samenwerken om onze systemen en daarmee onze klanten en collega's naar behoren te kunnen beschermen.

Voor een goede samenwerking vragen wij u:

- Uw bevindingen te mailen naar responsible-disclosure@conclusion.nl. Versleutel bij voorkeur uw bevindingen met onze PGP key om te voorkomen dat de informatie in verkeerde handen valt. Zoals u weet is versleuteling verplicht in geval u meldingen verstuurt die betrekking hebben op persoonsgegevens .
- De gevonden kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan noodzakelijk is om de kwetsbaarheid aan te tonen noch om gegevens van derden in te kijken, te verwijderen en/of aan te passen.
- Niet op onevenredige wijze te handelen door gebruik te maken van social engineering om u op deze wijze toegang te verschaffen tot het systeem, door een eigen backdoor in het systeem te plaatsen om vervolgens daarmee de kwetsbaarheid aan te tonen, aangezien daarmee aanvullende schade kan worden aangericht en onnodige veiligheidsrisico's worden gelopen, door een kwetsbaarheid verder uit te nutten dan noodzakelijk is om de kwetsbaarheid vast te stellen, door herhaaldelijk toegang tot het systeem te verkrijgen of de toegang te delen met anderen, door gebruik te maken van het zogeheten 'bruteforcen' van toegang tot systemen, daarbij is immers geen sprake van een kwetsbaarheid, maar alleen van het herhaaldelijk proberen van wachtwoorden.
- De kwetsbaarheid niet met derden te delen noch tot externe berichtgeving over te gaan en alle vertrouwelijke gegevens die zijn verkregen via deze kwetsbaarheid zo spoedig mogelijk te vernietigen na bevestiging van de melding.
- Voldoende informatie te geven om de kwetsbaarheid zo snel mogelijk op te kunnen lossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan uiteraard meer informatie nodig zijn.

Voor een goede samenwerking beloven wij u:

- Binnen 3 werkdagen te reageren op uw melding met onze inhoudelijke reactie op de melding en een datum waarbinnen de mogelijke kwetsbaarheid wordt opgelost.
  Geen juridische stappen tegen u te ondernemen, in het geval u zich aan bovenstaande voorwaarden heeft gehouden.
  Conclusion is wettelijk verplicht zich te houden aan de Wet Bescherming Persoonsgegevens en de Meldplicht Datalekken en werkt uiteraard mee aan eventuele vervolgacties vanuit de wetgever.
- Om uw melding vertrouwelijk te behandelen en uw persoonlijke gegevens niet zonder uw toestemming met derden te delen, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen, wordt u in dit geval op de hoogte gebracht). Melden onder een pseudoniem of via een tussenpersoon is mogelijk,
- Om u op de hoogte te houden van de voortgang van het oplossen van de mogelijke kwetsbaarheid.

- Om in eventuele berichtgeving over de gemelde kwetsbaarheid u indien u dit wenst, te vermelden als ontdekker van de kwetsbaarheid..
- Als dank voor uw melding bieden wij u een passende beloning aan.

Wij danken u bij voorbaat voor de samenwerking.