

Responsible disclosure-beleid

Responsible Disclosure Policy

Sagènn Groep

Responsible disclosure-beleid

Bij Sagènn vinden wij de veiligheid van onze systemen en applicaties 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 of applicaties 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 Ciso@Sagenn.nl . Indien mogelijk verzoeken we u om uw bevindingen te versleutelen 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 niet met anderen te delen totdat het is opgelost 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 op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden,
- 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.
- Een gevonden kwetsbaarheid op een domein niet op andere (sub)domeinen van Sagènn als nieuwe kwetsbaarheid te melden.
- Alleen kwetsbaarheden gevonden op Sagènn.nl worden behandeld.

Wat wij beloven:

- Wij reageren binnen 5 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,
- 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.

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.

Het Responsible Disclosure-beleid is gebaseerd op het beleid zoals gepubliceerd op responsibledisclosure.nl.

Responsible Disclosure Policy

At Sagènn, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to ciso@sagenn.nl . Encrypt your findings using our [PGP key](#) to prevent this critical information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
- A vulnerability found on one domain should not be reported as a new vulnerability on other (sub)domains of Sagènn.
- Do not scan other domains than Sagenn.nl. Only reports regarding Sagenn.nl will be processed.

What we promise:

- We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The reward will be determined based on the severity of the leak and the quality of the report.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

This Responsible Disclosure Policy document is based on the policy as published by responsibledisclosure.nl