Responsible Disclosure SVHW

SVHW vindt de beveiliging van zijn systemen erg belangrijk. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat er een zwakke plek in de systemen zit. Vindt u een zwakke plek in één van onze systemen? Laat ons dit dan weten, dan kunnen wij snel gepaste maatregelen nemen. Door het maken van een melding gaat u akkoord met onderstaande afspraken over Responsible Disclosure en handelt SVHW uw melding volgens onderstaande afspraken af.

SVHW vraagt het volgende van u:

- Stuur uw bevindingen per e-mail naar cert@svhw.nl, versleuteld met onze publieke PGP-sleutel om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren. Zo kunnen wij het zo snel mogelijk 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.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperkt u zich daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid. Vermijd dat uw advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Laat uw contactgegevens achter zodat wij contact met u kunnen opnemen om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter. Het staat u vrij om daarbij anoniem te blijven.
- Dien de melding alstublieft zo snel mogelijk in na het ontdekken van de kwetsbaarheid.
- Maak het probleem niet openbaar en deel het niet met anderen. Zo kan SVHW eerst maatregelen treffen. Ook als het niet mogelijk blijkt om het probleem adequaat op te lossen, vragen wij u het niet openbaar te maken of met anderen te delen.
- Wis eventueel verkregen (vertrouwelijke) gegevens zo snel mogelijk.

De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen;
- Het zogeheten 'bruteforcen' van toegang tot onze systemen;
- Het gebruik maken van social engineering;
- Misbruik maken van het probleem: Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden, zijn niet toegestaan. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan;
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen);
- Maak geen gebruik van tooling die bij SVHW overlast kunnen veroorzaken.

Wat mag u verwachten:

- Wij sturen u binnen één werkdag een ontvangstbevestiging van de melding.
- Wij reageren binnen drie werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel een verwachte datum voor een oplossing.

Responsible Disclosure SVHW

- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder zijn/haar toestemming, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij besteden geen publieke aandacht aan meldingen. Alleen als er een meldplicht (datalekken) geldt en de wet dit voorschrijft. De melder kan anoniem blijven. Wel kunnen wij de melding delen met de Informatie Beveiligingsdienst voor gemeenten (IBD). Zo borgen wij dat bij de IBD aangesloten organisaties hun ervaringen op dit vlak met elkaar delen. De melder kan anoniem blijven.
- Wij kunnen u een beloning bieden als dank voor uw hulp als het gaat om een ons nog onbekend en serieus beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het beveiligingsprobleem en de kwaliteit van de melding.