



Proces en afspraken voor het melden van een beveiligingslek

Wij hechten veel belang aan de beveiliging van onze systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer je een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding verklaar jij je als melder akkoord met onderstaande afspraken over Responsible Disclosure en zullen wij je melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van jou:

- Mail je bevindingen naar security@ssc-ons.nl
- Versleutel de bevindingen als dat mogelijk is met PGP om te voorkomen dat de informatie in verkeerde handen valt, of verzend het via <https://cryptshare.zwolle.nl/>
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres, de URL, screenshots van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij complexere kwetsbaarheden kan meer nodig zijn.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperk je daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de geconstateerde kwetsbaarheid en vermijd dat je advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Laat contactgegevens achter zodat we contact op kunnen nemen en samen een veilig resultaat kunnen bereiken. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding a.u.b. zo snel mogelijk in na ontdekking van de kwetsbaarheid.

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 systemen,
- behalve voor zover dat strikt noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekort schiet, dat wil zeggen als het buitengewoon eenvoudig is om met openbaar verkrijgbare en goed betaalbare hardware en software een wachtwoord te kraken waarmee het systeem ernstig kan worden gecompromitteerd.
- Het gebruik maken van social engineering.

- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem vóórdat het probleem is opgelost.
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar je door de kwetsbaarheid toegang toe hebt gehad. In plaats van een complete database te kopiëren, kun je normaliter volstaan met bijvoorbeeld een directory listing. 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 ((D)DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Dit mag je van ons verwachten:

- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Mogelijk delen wij de ontvangen melding (altijd anoniem) met de partners waarvoor wij werken en de Informatiebeveiligingsdienst voor gemeenten (IBD).
- In onderling overleg kunnen we, indien je dit wenst, je naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijf je anoniem.
- Wij sturen je binnen 3 werkdagen een ontvangstbevestiging.
- Wij reageren binnen 5 werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel een verwachte datum voor een oplossing.
- Wij lossen het door jou gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om je goed op de hoogte te houden van de voortgang en nooit langer dan 90 dagen te doen over het oplossen van het probleem. Wij zijn daarbij vaak wel mede afhankelijk van toeleveranciers.
- In onderling overleg kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.