Proces en afspraken voor het melden van een beveiligingslek

Responsible Disclosure

Het Shared Service Centrum ONS (SSC Ons) hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over Responsible Disclosure en zal het SSC Ons uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van u:

- Mail uw bevindingen naar security@ssc-ons.nl
  Versleutel s.v.p. de bevindingen om te voorkomen dat de informatie in verkeerde handen valt.
- Versleutel de bevindingen als dat mogelijk is met PGP om te voorkomen dat de informatie in verkeerde handen valt, of verzend het via https://app.zivver.com/l/start/a5c426ae-4f87-43e3-8d04-7351e5bfdd1d
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres, de URL, screenshots enzovoorts 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 en vermijd dat uw advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. 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 u door de kwetsbaarheid toegang toe heeft gehad. In plaats van een complete database te kopiëren, kunt u 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.

Wat u mag 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 u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft u anoniem.
- Wij sturen u 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 u gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om u 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.