Responsible Disclosure

Invior hecht veel belang aan de beveiliging van zijn systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in onze systemen te vinden is. Wanneer je een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag zo snel mogelijk, zodat we snel gepaste maatregelen kunnen nemen.

Zwakke plekken kunnen op twee manieren worden ontdekt: je loopt per ongeluk ergens tegenaan bij normaal gebruik van de digitale omgeving, of je doet expliciet je best om een zwakke plek te vinden. Ons Responsible Disclosure-beleid is geen uitnodiging om ons bedrijfsnetwerk uitgebreid te scannen op zwakke plekken.

Door het maken van een melding verklaar je jezelf, als melder, akkoord met onderstaande afspraken over Responsible Disclosure en zal uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van jou:

- Mail je bevindingen naar info@invior.nl.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk op kunnen lossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij complexere kwetsbaarheden kan meer informatie 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 door jou geconstateerde kwetsbaarheiden en vermijd dat je advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Contactgegevens achter te laten, zodat we met jou in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal een e-mailadres of telefoonnummer achter.
- De kwetsbaarheid zo snel mogelijk na ontdekking te melden.

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 zo strikt noodzakelijk is om aan de 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’, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat medewerkers met toegang tot gevoelige gegevens in het algemeen (ernstig) tekortschieten in hun plicht om daar zorgvuldig mee om te gaan. Dat wil zeggen als het op een volkomen legale wijze (dus niet via chantage of iets dergelijks) in het algemeen te eenvoudig is om hen over te halen tot het verstrekken van dergelijke gegevens aan onbevoegden. Je dient daarbij alle zorg te betrachten die redelijkerwijs van jou verwacht kan worden om de betreffende medewerkers zelf niet te schaden. Jouw bevindingen dienen uitsluitend gericht te zijn op het aantonen van kennelijke gebreken in de procedures en werkwijze binnen Invior en niet op het schaden van individuele personen die bij Invior werkzaam zijn.
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het 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 op kopiëren) van vertrouwelijke gegevens waar je door de kwetsbaarheid toegang tot hebt gekregen. In plaats van een complete database te kopiëren, kan je normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in onze systemen is nooit toegestaan.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of service wordt verminderd ((D)DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Wat je mag verwachten:

- Indien je aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen je doen en ook geen civielrechtelijke zaak tegen je aanspannen.
- Als blijkt dat je een bovenstaande voorwaarde toch hebt geschonden, kan Invior alsnog besluiten om gerechtelijke stappen tegen je te ondernemen.
- Wij behandelen een melding vertrouwelijk en delen persoonlijke van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij delen de ontvangen melding altijd met Internetbureau Forwart. In onderling overleg kunnen we, indien gewenst, de naam vermelden van de melder als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft de melder altijd anoniem.
- Invior reageert binnen vijf 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 beveiligingsproblemen 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. We 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.
- Wij kunnen je een bedankje bieden afhankelijk van de aard en omstandigheden. Het moet hierbij wel gaan om een nog onbekend en serieus beveiligingsprobleem.
- We streven ernaar om alle problemen zo snel mogelijk op te lossen, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over het probleem, nadat het is opgelost.