provincie limburg

Beleid Responsible Disclosure Provincie Limburg

Provincie Limburg vindt de beveiliging van haar systemen en informatievoorziening erg belangrijk. Ondanks onze zorg voor de beveiliging kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar: cert@prvlimburg.nl
- Voldoende informatie te geven om het probleem te reproduceren zodat we 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.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Wij vragen u om minimaal uw e-mail adres en/of telefoonnummer achter te laten.
- De melding zo snel mogelijk na ontdekking van de kwetsbaarheid te doen.
- De informatie over het beveiligingsprobleem niet met anderen te delen totdat het is opgelost.
- Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan noodzakelijk is om het beveiligingsprobleem aan te tonen.

Vermijd dus in elk geval de volgende handelingen:

- Het plaatsen van malware.
- Het kopiëren, wijzigen of verwijderen van gegevens in een systeem (een alternatief hiervoor is het maken van een directory listing van een systeem).
- Het aanbrengen van veranderingen in het systeem.
- Het herhaaldelijk toegang tot het systeem verkrijgen of de toegang delen met anderen.
- Het gebruik maken van het zogeheten “bruteforcen” van toegang tot systemen.
- Het gebruik maken van denial-of-service of social engineering.

Wat u mag verwachten:

- Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ict-systeem van Provincie Limburg aan alle bovenstaande voorwaarden voldoet, zullen we geen juridische consequenties verbinden aan deze melding.
- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.
- In onderling overleg kunnen we, indien u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.
- Wij sturen u binnen 1 werkdag een ontvangstbevestiging.
- Wij reageren binnen 5 werkdagen op een melding met de beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- Wij lossen het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk op. In onderling overleg kan worden bepaald of en op welke wijze over het probleem, nadat het is opgelost, wordt gepubliceerd.

Wat doen we met door ons aangetroffen kwetsbaarheden bij anderen:

- Provincie Limburg voert alleen onderzoek uit naar lekken in door derden beheerde systemen (onze samenwerkingspartners of leveranciers) na uitdrukkelijke toestemming hiervoor.
- Wij behouden ons het recht voor zonder voorafgaande kennisgeving onderzoek naar kwetsbaarheden uit te voeren op door derden aan de Provincie geleverde systemen en software als deze door ons zelf worden gehost en beheerd.
- Wij brengen zelf geen beveiligingslekken in software of systemen van derden in de publiciteit.
- Wij zullen door ons geconstateerde zwakke plekken z.s.m. melden aan de partij die verantwoordelijk is voor de hosting en/of het beheer van de systemen en software.
- Bij kwetsbaarheden in door de Provincie zelf gehoste en beheerde systemen en software brengen wij de leverancier hiervan op de hoogte.
- Door ons aangetroffen lekken of kwetsbaarheden worden tegelijkertijd ook bij het Nationaal Cyber Security Center van de Nederlandse overheid gemeld.