Responsible Disclosure

Bijgewerkt: augustus 2023

Bij de NOS vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen en gegevens kan het gebeuren dat er toch een zwakke plek is. Indien u een kwetsbaarheid in één van de ICT-systemen van de NOS heeft gevonden, hoort de NOS dit graag. Zo kunnen wij zo snel mogelijk de benodigde maatregelen nemen om dit te verhelpen.

De NOS hanteert voor dergelijke meldingen '*Responsible Disclosure*' principes. Dat betekent dat als u verantwoord met de kwetsbaarheid om zult gaan (zoals hieronder beschreven), de NOS daar iets tegenover stelt.

Hieronder treft u de afspraken aan die melder en de NOS zullen hanteren:

Wij vragen u:

- Uw bevindingen te mailen naar **informatiebeveiliging@nos.nl**. Om te voorkomen dat informatie in verkeerde handen valt, kan het bericht versleuteld worden. Gebruik hierbij onze publieke PGP sleutel, te vinden op https://pgp.surfnet.nl.
- Voldoende informatie te geven om het probleem te reproduceren, zodat de NOS het zo snel mogelijk kan 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.
- De melding zo snel mogelijk na ontdekking van de kwetsbaarheid te doen.
- Schriftelijk te bevestigen dat u conform deze 'Responsible Disclosure' hebt gehandeld en zult blijven handelen.
- De informatie over het beveiligingsprobleem niet met anderen te delen.
- Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan noodzakelijk om het beveiligingsprobleem aan te tonen.
- Juiste contactgegevens achter te laten, zodat de NOS met u in contact kan treden om samen te werken aan een veilig resultaat. Indien u hiervoor kiest, laat minimaal uw naam, e-mailadres en/of telefoonnummer achter. Anoniem melden of melden onder een pseudoniem is mogelijk.

Vermijd dus in elk geval de volgende handelingen:

- Het plaatsen van malware.
- Het kopiëren, wijzigen of verwijderen van gegevens in 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 geautomatiseerde scantools.
- Het gebruik maken van het zogeheten "bruteforcen" van toegang tot systemen.
- Het gebruik maken van denial-of-service of social engineering.

Wat wij beloven:

- Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ICT-systeem van de NOS aan bovenstaande voorwaarden voldoet, zal de NOS geen juridische consequenties verbinden aan deze melding.
- De NOS zal de melding onderzoeken. Geef ons hiervoor de tijd. Wij reageren zo spoedig mogelijk op een melding.
- De NOS behandelt een melding vertrouwelijk en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.
- Indien de contactgegevens bekend zijn, houdt de NOS de melder op de hoogte over de beoordeling van de melding en de voortgang van het oplossen van het probleem.
- De NOS lost het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk op.
- De NOS biedt een beloning als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning oplopen tot maximaal een bedrag van € 50 aan cadeaubonnen. Het moet hierbij wel gaan om een voor de NOS nog onbekend en serieus beveiligingsprobleem. Om hiervoor in aanmerking te komen, dienen wel uw contactgegevens bij de NOS bekend te zijn.