Responsible Disclosure

Nederlandstalige handleiding

nederlandse
publieke
omroep

Juni 2019, definitieve versie
Informatiebeveiliging – tussen het publiek met betrouwbare informatie

Inleiding

Voor de Nederlandse Publieke Omroep is het essentieel dat de systemen veilig zijn. Daarom doen we ons uiterste best om te zorgen voor een goede, deugdelijke beveiliging ervan. Toch kan het gebeuren dat er zwakke plekken in de beveiliging zitten en dat onze systemen daardoor kwetsbaar zijn.

De NPO moedigt doormiddel van Responsible Disclosure ('verantwoorde openbaarmaking') beleid de ontdekkers van zwakke plekken en kwetsbaarheden aan deze te melden aan de NPO. Wij kunnen dan passende maatregelen treffen om de gevonden kwetsbaarheid te verhelpen. Daarmee draag jij bij aan het veilig houden en maken van de NPO systemen. We vragen je om verantwoord met eventuele bevindingen om te gaan; de NPO zet daar dan wat tegenover. Denk aan een vermelding in de NPO Hall of Fame of een kleine vergoeding.

Hoe meld ik een bevinding?

- Stuur een email, zo snel mogelijk na de ontdekking, naar informatiebeveiliging@npo.nl, het liefst beveiligd met behulp van de gepubliceerde PGP sleutel.
- Geef voldoende informatie aan ons om de bevinding te kunnen reproduceren
  Denk aan het IP adres of de URL van het kwetsbare systeem en een duidelijke omschrijving van de gevonden kwetsbaarheid. Uiteraard mag de beschrijving bij complexere kwetsbaarheden uitgebreider zijn. Het zou mooi zijn als je ons precies kunt vertellen hoe we het probleem kunnen reproduceren.
- Laat juiste en voldoende contactgegevens achter: minimaal je naam, email-adres en een telefoonnummer. Wij behandelen je persoonsgegevens verantwoord en in lijn met het NPO privacy beleid.
- Bevestig schriftelijk (per email) dat je akkoord gaat met de principes uit het NPO "Responsible Disclosure" beleid om verantwoord om te gaan met de kwetsbaarheid. Zie volgende pagina.

Hoe ga ik verantwoord om met een gevonden kwetsbaarheid?

- Je deelt de informatie over het gevonden probleem en/of de kwetsbaarheid niet met anderen.
- Kennis over het gevonden probleem en/of de kwetsbaarheid gebruik je niet om handelingen te verrichten die verder gaan dan noodzakelijk om het probleem aan te tonen.

Het volgende doe je dus niet op en/of via kwetsbare NPO systemen:

- Plaatsen of verspreiden van welke vorm van malware, virussen, etc. dan ook.
- Veranderingen aanbrengen;
- Herhaaldelijk toegang verkrijgen of de toegang delen met anderen;
- Gebruikmaken van geautomatiseerde scantools;
- Het geforceerd (brute-force) toegang proberen te verkrijgen;
- Inzetten van een vorm van Denial of Service (DoS) aanvallen;
- Toepassen van social engineering technieken.

Wat kun je verwachten van de NPO?

Vrijwaring: Indien je een kwetsbaarheid meldt volgens het NPO Responsible Disclosure beleid, dan verbindt de NPO daar geen juridische consequenties aan.

Vertrouwelijkheid: De NPO behandelt je melding vertrouwelijk en deelt persoonlijke gegevens niet zonder jouw toestemming met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.

Waardering: De NPO waardeert je hulp en bedankt je daarvoor, eventueel met een beloning. Afhankelijk van een aantal factoren, zoals ernst, complexiteit, kwaliteit van de melding, etc., beoordeelt de NPO hoe de beloning er uit ziet. Dit varieert van een vermelding in de Hall of Fame tot een maximum van 50 EURO aan cadeaubonnen. Voorwaarde is dat er een voor de NPO onbekende en serieuze kwetsbaarheid en/of tekortkoming is gemeld.

Openheid en transparantie: De NPO houdt je op de hoogte over de beoordeling van de melding en de voortgang van het oplossen van het probleem. We lossen het door jou geconstateerde beveiligingsprobleem uiteraard zo snel mogelijk op.