Coordinated Vulnerability Disclosure (CVD)

Procedure

Colofon

Over Coördinated Vulnerability Disclosure

Hackers die gedreven door nieuwsgierigheid lekken vinden in de IT-systemen van organisaties, bevinden zich vaak in een juridisch grijs gebied. Ook al hebben ze geen kwade bedoelingen, het is vaak niet aantrekkelijk om de instelling te informeren over het lek. Organisaties pakken meldingen niet altijd op en het gebeurt soms dat een melder te maken krijgt met strafrechtelijke gevolgen. Dit beleid geeft helderheid over de spelregels voor de melder en over hoe Deltion een melding oppakt en afhandelt.

Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze IT-beveiliging. Daarmee kunnen we mogelijke schade voorkomen en we kunnen ervan leren. Het beleid Coördinated Vulnerability Disclosure regelt de voorwaarden en werkwijze rondom melding en afhandeling van kwetsbaarheden.

Doelstelling

- De mogelijkheid bieden om op ethisch verantwoorde wijze kwetsbaarheden in de systemen van Deltion onder de aandacht te brengen
- Het verbeteren van kwetsbaarheden in onze systemen

Bestemd voor

Voor geïnteresseerden (openbaar document).

Samenstelling en beheer

Dit document is verstrekt onder de creative commons-licentie CC3.0 en is gebaseerd op de tekst door Floor Terra (responsibledisclosure.nl). Het sluit aan bij het model IBPDOC27 (saMBO-ICT).

Versiebeheer

Versie	Door	Datum	Wijziging/actie
1.0	Niels Dutije	9 juni 2017	Initieel document
1.1	Helma de Boer	20 mei 2020	Actualiseren, certificaat, Hall of Fame + Engelse versie
1.2	Helma/René	29-06-2020	Kleine tekstuele foutjes hersteld
2.0	Helma	06-07-2020	Beperking scope en akkoord JK/CIO
3.0	Hans Hoeven	21-09-2022	Naamswijziging en uitbreiding van uitzonderingen

1. Coördinated Vulnerability Disclosure

Deltion vindt de veiligheid van haar systemen en het verhelpen van kwetsbaarheden in die systemen belangrijk. Ondanks onze zorg voor de beveiliging van de systemen kan het voorkomen dat er toch een zwakke plek is. We werken daarin graag samen met degene die een kwetsbaarheid ontdekt en/of bij ons meldt. Dit beleid wordt op onze website gepubliceerd in Nederlands en Engels.

Wij vragen van de melder:

- De bevindingen te mailen naar csirt@deltion.nl. Versleutel gevoelige informatie eventueel om te voorkomen dat de informatie in verkeerde handen valt.
- Voldoende informatie te geven om het probleem te reproduceren, zodat wij 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.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken of te veranderen of verwijderen en extra voorzichtig te zijn bij persoonsgegevens.
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen direct te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, applicaties van derden, social engineering, distributed denial of service of spam, of op een andere manier ons netwerk uitgebreid actief te onderzoeken/scannen op kwetsbare plekken. Deltion monitort het netwerk en de kans is groot dat de scan of aanval wordt gedetecteerd en dat er vervolgens onnodige kosten worden gemaakt.
- Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan strikt noodzakelijk zijn om de kwetsbaarheden aan te tonen.
- Geen schadelijke handelingen te verrichten zoals: plaatsen van malware, kopiëren, wijzigen of verwijderen van gegevens in een systeem, het aanbrengen van veranderingen in het systeem, herhaaldelijk toegang tot het systeem verkrijgen of de toegang delen met anderen.

Wij beloven aan de melder:

- Deltion neemt geen juridische stappen tegen de melder als hij/zij zich houdt aan de bovenstaande voorwaarden.
- Wij reageren binnen vijf dagen op een melding.
- Wij houden de melder op de hoogte van de voortgang van het oplossen van het probleem,
- Wij behandelen een melding vertrouwelijk en delen geen persoonlijke gegevens van de melder met derden zonder zijn/haar toestemming, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Anoniem of onder een pseudoniem melden is mogelijk.
- In berichtgeving over het gemelde probleem vermelden wij de naam van de melder als de ontdekker (als hij/zij dat wenst).
- Wij vermelden de melder met naam of nickname in onze online Hall of Fame als hij/zij zich daarvoor bij ons bekend heeft gemaakt en op verzoek verstrekken we een certificaat.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en alle betrokken partijen op de hoogte te houden over de voortgang. Deltion wordt graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Beperkte scope

Deltion geeft geen beloning voor triviale kwetsbaarheden.

Hieronder staan voorbeelden van bekende en geaccepteerde kwetsbaarheden en risico's die niet in scope zijn bij de procedure Coordinated Vulnerability Disclosure:

- HTTP 404-codes/pagina's of andere HTTP-codes/pagina's en Content Spoofing/tekstinjectie op deze pagina's.
- Fingerprinting/versievermelding op gemeenschappelijke/openbare diensten.
- Publieke bestanden of mappen met niet-gevoelige informatie, (bijvoorbeeld robots.txt).
- Clickjacking en problemen die alleen misbruikt kunnen worden door clickjacking.
- Gebrek aan Secure/HTTPOnly vlaggen op niet-gevoelige cookies.
- OPTIONS HTTP method ingeschakeld.
- Host header injection.
- Alles gerelateerd aan HTTP-beveiligingsheaders, bijvoorbeeld:
  - Strict-Transport-Security
  - X-Frame-Options
  - X-XSS-Protection
  - X-Content-Type-Options
  - Content-Security-beleid
- Problemen met SSL-configuraties:
  - SSL-forward secrecy uitgeschakeld
  - Zwakke/onveilige cipher suites
- Problemen met SPF, DKIM of DMARC.
- Ontbrekende DNSSEC-informatie.
- Melding van verouderde software of upgrade mogelijkheid zonder de daarbij behorende proof of concept van een werkende exploit te delen.
- Systemen en protocollen die misbruikt kunnen worden voor een DDoS aanval.
- Opzettelijke directory inhoud listing(s) voor onderzoek of publicatie doeleinden.
- Informatieblootstelling in metadata.

2. Evaluatie

Controle naleving en evaluatie

De naleving van deze werkwijze wordt periodiek gecontroleerd. Eveneens wordt periodiek gecontroleerd of de afspraken en de werkwijze in dit document nog actueel zijn of moeten worden bijgesteld, geïnitieerd door het team Privacy & Security.