Responsible Disclosure

VLOT LOGISTICS vindt het belangrijk dat onze ICT-systemen en websites veilig zijn en streeft een hoge beveiliging daarvan na. Toch kan het gebeuren dat er een zwakke plek in één van deze systemen voorkomt.

Indien u een zwakke plek in één van onze websites of ICT-systemen heeft gevonden, horen wij dit graag van u. Uw melding stelt ons in staat om direct de noodzakelijke maatregelen te nemen om de gevonden kwetsbaarheid te verhelpen.

Wij hanteren voor meldingen de zogenaamde 'Responsible disclosure' principes. Dat heeft als gevolg dat bij verantwoord handelen en omgaan met gevonden kwetsbaarheden, wij dit erg waarderen en ook zullen belonen.

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

VLOT LOGISTICS vraagt van de melder:
Uw bevindingen te mailen naar security@vlotLogistics.nl. Versleutel de bevindingen indien mogelijk om te voorkomen dat de informatie in verkeerde handen valt. Public PGP Key
Voldoende informatie geven om het probleem te reproduceren, zodat VLOT LOGISTICS 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.
Juiste contactgegevens achter te laten, zodat wij met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal naam, een email adres en/of telefoonnummer achter.
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.
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 gebruikmaken van geautomatiseerde scantools.
- Het gebruik maken van het zogeheten "bruteforcen" van toegang tot systemen.
- Het gebruik maken denial-of-service of social engineering.
- Wat u mag van ons verwachten?
- Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ICT-systeem

VLOT LOGISTICS aan bovenstaande voorwaarden voldoet, zal VLOT LOGISTICS geen juridische consequenties verbinden aan deze melding.

- VLOT LOGISTICS 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.
- VLOT LOGISTICS vraagt u schriftelijk te bevestigingen dat u conform deze 'Responsible Disclosure' hebt gehandeld en zult blijven handelen, en vraagt om uw contactgegevens voor zover die nog niet bekend waren.
- VLOT LOGISTICS houdt de melder op de hoogte over de beoordeling van de melding en de voortgang van het oplossen van het probleem.
- VLOT LOGISTICS lost het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk op.

Wat Vlot Logistics beloofd:

- Wij reageren binnen 5 dagen op uw melding en zullen u op de hoogte houden van de voortgang met betrekking tot de oplossing van het probleem;
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen;
- Indien er berichtgeving over het gemelde probleem verschijnt zullen wij dit met u afstemmen en eventueel uw naam vermelden als ontdekker;
- een beloning als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren. Passend bij de wensen van de melder, en op basis van redelijkheid, zullen we de beloning, na melding en onderzoek, verder met u afstemmen.
- Voorwaarde is wel dat het een voor de VLOT LOGISTICS een nog onbekend en serieus beveiligingsprobleem betreft.

Out-of-Scope Vulnerabilities

- Social engineering attacks, including those targeting internal employees
- Physical attacks against our infrastructure, facilities and offices
- Scanner output or scanner-generated reports, including any automated or active exploit tool
- Any vulnerability obtained through the compromise of employee account
- Network Vulnerabilities:
- Account takeover (PLA, User enumeration, etc)
- Spam
- Clickjacking, Login/logout CSRF
- Fingerprinting, error message disclosure
- Protocol level attacks (e.g BEAST/BREACH)
- Lack of security headers, httponly flags, etc