Responsible disclosure beleid

Trans Link Systems B.V. (Translink) draagt met de OV-chipkaart eraan bij dat reizigers elke dag veilig en makkelijk reizen met het openbaar vervoer. De beveiliging van de OV-chipkaart heeft de hoogste prioriteit bij Translink. Uiteraard vindt Translink het ook belangrijk dat de eigen ICT-systemen veilig zijn. Elke dag werken specialisten aan het optimaliseren van de systemen en processen. Toch kunnen kwetsbaarheden ook in onze systemen voorkomen. Ontdekt u kwetsbaarheden in onze systemen of OV-chipkaart? Dan werken we graag samen met u aan een oplossing.

Welke kwetsbaarheden kan ik melden?
U kunt problemen melden die te maken hebben met onze online dienstverlening of OV-chipkaart. Bijvoorbeeld:

- Cross site scripting
- SQL-injectie
- Encryptie

Goed om te weten: het meldpunt is niet bedoeld voor klachten over de dienstverlening van Translink, beschikbaarheid van de website of de app. U kunt hiervoor ons contactformulier gebruiken. Het is ook niet bedoeld voor meldingen over problemen met OV-chipkaartapparatuur op (trein/metro) stations of in (bus/tram) voertuigen. Hiervoor verwijzen wij u naar de betreffende vervoerder.

Hoe doe ik een melding?
Mail ons via responsible.disclosure@translink.nl en maak daarbij gebruik van onze publieke PGP Key. Zet in een mail:

- Een uitgebreide beschrijving van het gevonden probleem.
- De benodigde informatie waarmee we de gevonden kwetsbaarheid zelf kunnen reproduceren en verifiëren.

PGP Key

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.4.9 (MingW32)

mQENBFPg3akBCADP38pon/G/YgRl31F7wo+Q73ODuxeT5Im14HQN09clBl/TJNYv
C2HDyQbWuw2lzvqv4+t6Hh6nQAOaSa4jIDUx/S7ZhlLSxqb/Kv7T30uU2DSSe697
5t5c9TupqFIVSMfDKrDkUU0X2eFUBDl/Hlujx5p9IDW1sfkqaH6HnA4H/M3Rv2r/
W7xF7m28Sz24M/XFvhUWU9LUcjtBulpF/oLO7IWR2mfv2zFsHc8sxBD1lV/7ATcb
yxQsCDYrLgVKC3NGNgeMllqxynaMnsYeXVg5o2TQH5hYkFu22L7Bewr+y6rsF5n/
KePA2BzWNMT3c3/ksLXpo+THm6Df0B1G0TqzABEBAAG0QFJlc3BvbnNpYmxlX0Rp
c2Nsb3N1cmVfVExTIDxyZXNwb25zaWJsZS5kaXNjbG9zdXJlQHRyYW5zbGluay5u
bD6JATYEEwECACAFAlPg3akCGw8GCwkIBwMCBBUCCAMEFgIDAQIeAQIXgAAKCRB6
ldXW1GS84oxyCACfNiFGFDh3+Vzq+JiHLs8RmjCn5xbD2Zb8TqvfDotyH6+Vvp7q
iAV5DucvFM99nQfcmyZoUucH2asCdiJUxLPx1WG5w0fDr2IOdYuzyqEaBqOdBT56
S3GP9oIA5238l7fg48pbyjlCEfHjq3FZUtZgMjB5V19ElzKeuWHXdoFdG6hvttMt
5IDmwL617e78TCc5G7ePdr8XRbbM/q/bB+RnMAdQ08jQKV5+lfgKcqsouQVVm8Nk
qW0ZqEDxFvDEokPfzmQH9V5uZ3z4LDF8lTqUyyVL88w3gwMv2QyL2xxNsANC/Q32
oFvPToPQXTFRIgh4U8st2DYdj6l0bNNzGLQn
=0ukB
-----END PGP PUBLIC KEY BLOCK-----

Translink bv
Stationsplein 151-157, 3818 LE Amersfoort
Postbus 1808, 3800 BV Amersfoort

T +31 33 467 20 00
F +31 33 467 20 99
E info@translink.nl

BTW NL810814341B01
KvK 30177126
IBAN NL21 RABO 0192 3003 34

www.translink.nl

Kan ik anoniem een melding doen?
U kunt natuurlijk ook een anonieme melding doen. Houd er rekening mee dat het dan niet mogelijk is om na de melding contact op te nemen. Of een eventuele beloning uit te keren. Om anoniem te blijven, mailt u vanaf een willekeurig e-mailadres zonder verdere contactgegevens te noemen.

Wat doet Translink met de melding?
Uw melding wordt onderzocht door onze beveiligingsexperts. Binnen twee werkdagen ontvangt u van ons informatie over:

- De beoordeling van uw melding;
- Of we een oplossing gaan toepassen;
- Wanneer we dat gaan doen.

De spelregels
Bij het melden van een kwetsbaarheid kunt u handelingen verrichten die strafbaar zijn. Handelt u integer, houdt u zich aan de spelregels en meldt u de kwetsbaarheid aan ons, dan is er voor ons geen aanleiding om aangifte te doen. Daarnaast komt u mogelijk in aanmerking voor een beloning.

- Iedereen die een mogelijke kwetsbaarheid in onze systemen ontdekt, kan een melding doen. Dus ook als u geen gebruikmaakt van een OV-chipkaart.
- We behandelen alleen Engelse of Nederlandse meldingen.
- Maak geen gebruik van aanvallen op fysieke beveiliging, van social engineering of distributed denial of service, spam of applicaties van derden.
- Plaats geen backdoor in een informatiesysteem om daarmee de kwetsbaarheid aan te tonen.
- Maak minimaal gebruik van een kwetsbaarheid. Doe alleen wat noodzakelijk is om de kwetsbaarheid vast te stellen.
- Wijzig of verwijder geen gegevens van het systeem.
- Maak geen kopieën van eventuele databases of bestanden. Een alternatief hiervoor is het maken van een ‘directory listing’ van een systeem.
- Breng geen systeemveranderingen aan.
- Probeer niet herhaaldelijk wachtwoorden (‘brute force’) om toegang tot systemen te krijgen.

Het onderzoeken naar of van een kwetsbaarheid mag nooit leiden tot:

- Financiële, juridische, operationele of imago schade van Translink.
- Verstoring van onze dienstverlening.
- Het openbaar maken van vertrouwelijke (klant-) gegevens.

Uw privacy
Als u een melding hebt gedaan, vragen we u om uw contactgegevens (naam, e-mail, publieke PGP-sleutel en eventueel telefoonnummer). We geven uw gegevens niet aan anderen en gebruiken ze niet voor andere doeleinden. Tenzij we daarvoor wettelijk worden verplicht, bijvoorbeeld bij vordering door justitie.

Mag ik de kwetsbaarheid die ik vind en mijn onderzoek openbaar maken?
Maak uw onderzoek of kwetsbaarheden in onze IT-systemen nooit openbaar zonder overleg met ons. Overleg met onze beveiligingsexperts en geef ons de tijd om het probleem op te lossen.

Beloning
We zijn blij met iedereen die ons helpt om onze systemen en processen te optimaliseren. Als dank daarvoor ontvangt u voor gemelde kwetsbaarheden, die daadwerkelijk door ons zijn verholpen of leiden tot verandering van de dienstverlening, een passende beloning. Translink beslist of u hiervoor in aanmerking komt en wat de grootte van de beloning is. Zijn er meerdere melders voor dezelfde kwetsbaarheid? Dan is de beloning voor de eerste melder.

Bekijk de Hall of Fame

Ons beleid rond het melden van kwetsbaarheden is gebaseerd op de leidraad van het Nationaal Cyber Security Centrum (NCSC).