RESPONSIBLE DISCLOSURE

1. RESPONSIBLE DISCLOSURE GELDSERVICE NEDERLAND

Om de systemen veilig en betrouwbaar te houden werkt Geldservice Nederland ('GSN') continu aan het optimaliseren van systemen en processen. Het kan desondanks voorkomen dat er toch nog kwetsbaarheden in de systemen aanwezig zijn. Heeft u een zwakke plek in een ICT-systeem ontdekt? GSN stelt het op prijs als u daar een melding van maakt. GSN heeft daarom een Responsible Disclosure Policy vastgesteld om meldingen te stimuleren.

2. KWETSBAARHEDEN VAN ICT-SYSTEMEN

U kunt alle soorten kwetsbaarheden in de ICT-systemen melden. Voorbeelden zijn: cross-scripting-kwetsbaarheden, SQL-injectie-kwetsbaarheden, encryptie-zwakheden. Deze Responsible Disclosure is niet bedoeld voor het melden dat de website niet beschikbaar is, het melden van fraude, het melden van phishing e-mails en spam en het melden van virussen.

3. SPELREGELS

Deze Responsible Disclosure is gebaseerd op de 'Leidraad Responsible Disclosure' van het Nationaal Cyber Security Centrum[1]. De volgende spelregels gelden bij het maken van een melding:

- U gebruikt bij uw onderzoek alleen methoden of technieken die nodig zijn voor het vinden of aantonen van de zwakheden en u maakt het probleem niet openbaar;
- U gebruikt geen social engineering om toegang te krijgen tot de systemen;
- U plaatst geen backdoor in een van de informatiesystemen om de zwakke plek te laten zien;
- U doet alleen wat strikt noodzakelijk is om de kwetsbaarheid aan te tonen;
- Er worden geen gegevens van de GSN systemen gekopieerd, gewijzigd of verwijderd. Stuur de minimale gegevens die u nodig heeft om het probleem aan te tonen, een alternatief hiervoor is het maken van een directory listing of een screenshot;
- U brengt geen veranderingen aan in het systeem;
- U beperkt de pogingen tot toegang tot het systeem, u deelt de toegang niet met anderen;
- U maakt geen gebruik van 'bruteforce attacks' om toegang tot de systemen te krijgen.

4. MELDING DOEN

U kunt de melding aan ons doorgeven via: [info@geldservicenederland.nl]. Omschrijf in uw e-mail uw bevindingen en leg uit welke stappen u ondernam en noem de volledige URL. Na ontvangst van de melding wordt er uiterlijk binnen 3 werkdagen contact met u opgenomen. Dat kan gaan over de door u gevonden zwakke punten, hoe u die heeft gevonden en over eventuele vervolgstappen.

[1] https://www.rijksoverheid.nl/documenten/richtlijnen/2013/01/03/leidraad-om-te-komen-tot-een-praktijk-van-responsible-disclosure

5. VOLGENS DE SPELREGELS

Het kan zijn dat u tijdens uw onderzoek handelingen uitvoert die strafbaar zijn. Wanneer u zich aan de bovenstaande spelregels houdt en u zorgvuldig en te goeder trouw handelt, zal GSN geen aangifte doen en geen schadeclaim indienen.
Dit vrijwaart u echter niet van de mogelijkheid dat de Officier van Justitie beslist om u te vervolgen. Hier gaat GSN niet over, of GSN nu aangifte doet of niet.

GSN stimuleert u om gevonden kwetsbaarheden te rapporteren, u kunt daarom mogelijk een beloning hiervoor ontvangen. GSN is hiertoe niet verplicht. Alleen als het een serieus beveiligingsprobleem betreft en u zorgvuldig en te goeder trouw volgens de spelregels heeft gehandeld kunt u een passende vergoeding krijgen als dank voor het meedenken. De hoogte van de vergoeding staat van te voren niet vast en wordt door GSN bepaald op basis van de ernst en omvang van het gemelde probleem. Beloningen worden niet toegekend indien blijkt dat er sprake is van misbruik of schending van de spelregels. Een beloning wordt niet uitgekeerd als de kwetsbaarheid al bij GSN bekend is. Kwetsbaarheden ontdekt door GSN medewerkers worden uitgesloten van beloning.

6. PRIVACY

GSN gebruikt uw persoonsgegevens alleen om actie te ondernemen naar aanleiding van uw melding. GSN zal uw persoonsgegevens niet met anderen delen behalve als dit voor GSN wettelijk verplicht is, bijvoorbeeld als justitie dit aan GSN vraagt. Of als GSN uw actie ziet als een strafbaar feit en u dus niet te goeder trouw heeft gehandeld, GSN zal in dat geval aangifte doen bij de politie.

* * * * *