Status: Definitief
Datum vastgesteld in CvB: 02-10-2017
Auteur: Rianne te Brake

Responsible Disclosure Universiteit Twente

Inleiding

Bij de Universiteit Twente vinden wij de veiligheid van uw en onze gegevens erg belangrijk, en daarom beveiligen wij onze systemen. Ondanks onze zorg kan het voorkomen dat er toch een zwakke plek is in deze beveiliging.

Heb je een zwakke plek in één van onze systemen gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om onze gebruikers en systemen beter te kunnen beschermen.

Wij vragen jou:

- Geen aanvallen uit te voeren op fysieke beveiliging en mensen (social engineering).
- Geen gebruik te maken van Distributed Denial of Service aanvallen of spam.
- Geen melding van '13-in-een-dozijn' te doen. Voorbeelden hiervan staan op de website onder Responsible disclosure.
- Je bevindingen te mailen naar responsible-disclosure@utwente.nl. Melden onder een pseudoniem is mogelijk. Indien je vindt dat de gegevens zo gevoelig zijn dat je ze wenst te versleutelen, verzoeken we je dat te melden. We zorgen er dan voor dat je een adres krijgt waar je PGP-versleutelde mail naar toe kunt sturen.
- 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.
- Alle vertrouwelijke gegevens die zijn verkregen via het lek zo snel mogelijk na het doorgeven van je melding te verwijderen, maar altijd na afstemming met ons om er zeker van te zijn dat wij het probleem kunnen reproduceren.
- 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, te verwijderen of aan te passen.
- Het probleem niet met anderen te delen totdat het is opgelost.
- Niet zelf over het opgeloste probleem te publiceren tenzij dit met ons is afgestemd.

Wat bij beloven:

- Wij vinden het belangrijk dat kwetsbaarheden zo snel mogelijk aan ons worden gemeld, zodat wij direct actie kunnen ondernemen om onze omgeving weer veilig te maken. Meldingen worden daarom door ons altijd in dank aanvaard. Wij zullen dan ook geen juridische stappen overwegen naar melders die zich ongeautoriseerd toegang hebben verschaft tot gevoelige informatie, mits je je hebt gehouden aan bovenstaande punten.
- Wij behandelen je melding vertrouwelijk en zullen jouw persoonlijke gegevens niet zonder je toestemming met derden delen tenzij dat noodzakelijk is om aan een wettelijke verplichting te voldoen.

- Wij reageren binnen 5 werkdagen op je melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij houden je op de hoogte van de voortgang van het oplossen van het probleem.
- Als je er prijs op stelt nemen we jou op als melder in de Hall of Fame, indien gewenst kan dit onder pseudoniem.
- Relevante inhoud van de opgeloste melding kunnen we publiceren op www.utwente.nl/cybersafety, tenzij er redenen zijn om dit niet te doen. Bijvoorbeeld wanneer de oplossing heeft geleid tot (ontdekking van) een gerelateerde kwetsbaarheid die nog niet is opgelost, of wanneer de publicatie kan leiden tot imagoschade voor (een onderdeel van) de UT.
- In berichtgeving over het opgeloste probleem zullen wij, indien je dit wenst, je naam vermelden als de ontdekker en melder.

Wij streven er naar alle gemelde problemen zo snel mogelijk op te lossen.