NL: CVD Coordinated Vulnerability Disclosure/ Responsible Disclosure procedure EN: see below

Veiligheid van informatie en systemen is van groot belang. Dat vindt ICT Teamwork ook en we werken daarom voortdurend aan het veilig houden van onze systemen. Toch kunnen er zwakke plekken bestaan of er gaat simpelweg iets mis. Mocht je zo'n zwakke plek/ kwetsbaarheid hebben gevonden, dan horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. De spelregels daarbij staan in deze CVD/ Responsible Disclosure procedure.

We vragen je om:

- alleen te doen wat strikt noodzakelijk is om de kwetsbaarheid aan te tonen,
- de kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is of gegevens (al dan niet van derden) in te kijken, verwijderen of aan te passen,
- bij het onderzoek van de gevonden kwetsbaarheid geen systemen of diensten te beschadigen, dus ook geen backdoor(s) plaatsen of niet gerelateerde wijzigingen in systemen doorvoeren,
- de beschikbaarheid van onze systemen niet te beïnvloeden of te onderbreken,
- geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, ddos, spam of applicaties van derden,
- je bevindingen te mailen naar security@ictteamwork.nl. Als je vertrouwelijke informatie wilt uitwisselen, overleg dan even met ons wat de beste manier is om dit te doen.
- na de melding de kwetsbaarheid niet opnieuw (proberen) te gebruiken.
- het probleem niet met anderen te delen totdat het is opgelost en om alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten ervan te wissen,
- 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.
- te reageren als wij je vragen om extra informatie rond de melding.

We beloven je dat:

- wij binnen 3 (werk-)dagen op je melding reageren met onze beoordeling van de melding en een verwachte datum voor een oplossing. Melden onder een pseudoniem is mogelijk.
- wij je melding vertrouwelijk behandelen en dat wij je persoonlijke gegevens niet zonder jouw toestemming met derden zullen delen tenzij dat wettelijk verplicht is of als wij een (meer dan) redelijk vermoeden hebben dat je niet te goeder trouw handelt.
- wij je op de hoogte houden van de voortgang van het oplossen van het probleem.
- wij in berichtgeving over het gemelde probleem wij je naam zullen vermelden als de ontdekker van het probleem (als je dat zou willen).
- wij geen aangifte zullen doen of andere juridische stappen tegen je zullen ondernemen betreffende de melding als je je hebt gehouden aan deze spelregels en je te goeder trouw en zorgvuldig hebt gehandeld op de manier die wij van je vragen,
- als dank voor je hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem waar wij zelf invloed op hebben en die volgens deze spelregels is verlopen. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding met een cadeaubon van maximaal € 300,-.
- wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

EN: CVD Coordinated Vulnerability Disclosure/ Responsible Disclosure procedure NL: zie hierboven

Security of information and systems is of great importance. ICT Teamwork agrees with this and we are therefore constantly working to keep our systems secure. Nevertheless, weaknesses can exist or sometimes things simply go wrong. If you have found such a weakness/ vulnerability, we would like to hear about it so that we can take measures as quickly as possible. The rules of the game are set out in this CVD/ Responsible Disclosure procedure.

Our request to you:

- do only what is strictly necessary to demonstrate the vulnerability,
- don't exploit the vulnerability by, for example, downloading more data than necessary or accessing, deleting or modifying data (third-party or otherwise),
- when investigating the vulnerability found, do not damage any systems or services, including placing backdoor(s) or making unrelated changes to systems,
- don't affect or interrupt the availability of our systems,
- don't use physical security attacks, social engineering, ddos, spam or third-party applications,
- send your findings by email to security@ictteamwork.nl. If you want to share confidential information, please consult us on the best way to do this.
- After notification, do not (try to) use the vulnerability again.
- don't share the problem with others until it is resolved and to delete all confidential data obtained through the leak immediately after it is closed,
- provide us with sufficient information to reproduce the problem so that we can resolve it as soon as possible. Usually, the IP address or URL of the affected system and a description of the vulnerability is sufficient, but more may be required for more complex vulnerabilities.
- Please respond if we ask you for additional information around the report.

Our promise to you:

- we respond to your report within 3 (working) days with our assessment of the report and an expected date for resolution. Reporting under a pseudonym is possible.
- we will treat your report confidentially and we will not share your personal data with third parties without your consent unless required to do so by law or if we have a (more than) reasonable suspicion that you are not acting in good faith.
- we will keep you updated on the progress of solving the problem.
- we will include your name as the discoverer of the problem (if you would like so) in notifications about the reported problem.
- we will not press charges or take any other legal action against you regarding the report if you have complied with these rules and acted in good faith and with due care in the manner we ask of you,
- as a thank you for your help, we offer a reward for every report of a security problem unknown to us that we can influence and that has been handled according to these rules. We determine the size of the reward based on the severity of the leak and the quality of the report with a gift voucher up to €300.
- We aim to resolve all problems as soon as possible and we are happy to be involved in any publication about the problem after it is resolved.