References/referenties

Responsible Disclosure (English)

Test-Correct is developed by The Teach & Learn Company B.V.

At The Teach & Learn Company B.V. , we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

For this, we have prepared the following Responsible Disclosure based on https://responsibledisclosure.nl/en/.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Responsible Disclosure is NOT for submitting complaints about The Teach & Learn Company B.V.'s services or the availability of our websites or services. Please use the usual support channels for that.

Please do the following:

- E-mail your findings to security@test-correct.nl. If anyway possible, encrypt your findings in a PGP encrypted PDF (see the end of the document for the PGP key) containing all information about the vulnerability and a generic e-mail without details of the vulnerability to prevent the information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
- Delete all confidential data obtained through the leak immediately after plugging the leak,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties,
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation,
- While investigating the vulnerability found, make sure you do not cause any damage,
- Your investigation must not lead to interruption of our online services or disclosure of confidential data,
- Do not insert a backdoor into a system. Not even to demonstrate the vulnerability. Placing a backdoor in a system makes that system even more insecure.
- Do not make system changes, and
- Do not try to penetrate a system more often than necessary. If you manage to penetrate a system, do not share the access with others.
- To qualify for a reward, the vulnerability must have the potential to seriously affect the confidentiality, integrity or availability of our service. To demonstrate this, we ask that you do not execute the vulnerability and cause damage, but to theoretically outline what the consequences of the vulnerability might be. The vulnerability must also not be known to us to qualify for a reward.

What we promise:

- We will respond to your report within 20 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,

- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission, unless necessary to comply with a legal obligation. Reporting under a pseudonym is possible,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (if desired), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate (fully anonymised) publication of the problem after it is resolved, if applicable.

Our PGP key can be found on the last page of this document.

Responsible Disclosure (Nederlands)

Test-Correct wordt ontwikkeld door The Teach & Learn Company B.V.

The Teach & Learn Company B.V. vindt de veiligheid van haar systemen erg belangrijk. Ondanks onze zorg voor de beveiliging hiervan kan het voorkomen dat er toch een zwakke plek is.

Hiervoor hebben wij de volgende Responsible Disclosure opgesteld op basis van https://responsibledisclosure.nl.

Als u een zwakke plek in een van onze systemen heeft gevonden horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Responsible disclosure is NIET bedoeld voor het indienen van klachten over de dienstverlening van The Teach & Learn Company B.V. of de beschikbaarheid van onze websites of diensten. Gebruik daarvoor de gebruikelijke support kanalen.

Wij vragen u:

- Uw bevindingen te mailen naar security@test-correct.nl. Indien mogelijk, versleutel uw bevindingen in een met PGP versleutelde PDF (zie einde document voor de publieke sleutel) met alle informatie over de kwetsbaarheid en een generieke mail zonder details van de kwetsbaarheid om te voorkomen dat de informatie in verkeerde handen valt,
- 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, verwijderen of aanpassen,
- Het probleem niet met anderen te delen totdat het is opgelost,
- Alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen,
- Geen gebruik te maken van aanvallen op fysieke beveiliging, bruteforce-technieken, social engineering, distributed denial of service, spam of applicaties van derden,
- 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,
- Zorg ervoor dat u tijdens het onderzoeken van de gevonden kwetsbaarheid geen schade aanricht,
- Uw onderzoek mag niet leiden tot onderbreking van onze online dienstverlening of het openbaar maken van vertrouwelijke gegevens,
- Plaats geen backdoor in een systeem. Ook niet om de kwetsbaarheid aan te tonen. Door het plaatsen van een backdoor in een systeem, wordt dat systeem nog onveiliger.
- Breng geen systeemveranderingen aan, en
- Probeer niet vaker dan nodig een systeem binnen te dringen. Als het lukt om een systeem binnen te dringen, deel de toegang dan niet met anderen.
- Om in aanmerking te komen voor een beloning, moet de kwetsbaarheid de vertrouwelijkheid, integriteit of beschikbaarheid van onze dienst ernstig kunnen aantasten. Om dit aan te tonen vragen wij om de kwetsbaarheid niet uit te voeren en eventuele schade aan te richten, maar theoretisch te schetsen wat de gevolgen kunnen zijn van de kwetsbaarheid. De kwetsbaarheid moet ook niet bekend bij ons zijn om in aanmerking te komen voor een beloning.

Wat wij beloven:

- Wij reageren binnen 20 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding,
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk,
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem,
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker, en
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding met een minimum van een waardebon van €50,-.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een (volledig geanonimiseerde) publicatie over het probleem nadat het is opgelost, indien van toepassing.

Onze PGP sleutel staat op de laatste pagina van dit document.

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

mQMuBGVlyI4RCAC24YrgNK0KYXu1OwddHBzNyGHXW0iSOA3+zA3Kkbm9ueFWhNLG
2iyre8E9W1ZXFOeIa7xx8/LLvQHLWOmq4w4qLeDAUZ1Pt6reBLdAPyeTqn/mer+k
+ae5/2kzEhSES87T34kH1Ivf4sjJFnib1EUardZL7SQu53iVlY7hC0HWAbXG571h
qjPe3H/2OgCgo3HAK53C9u2ilmAB5vP7YsLPoop2jqLNAW/yJCxcXu5sBMrqaWj+
TI8oIq29iQI6B+tjkJx0g06I9pvOIMfmLPjSr5RhIvEnyDB3uolhTnyHaOkohVRF
uc5ZA4QtIRB6zMhymNy7t6y8ZpFcMQDlpY5bAQDEcEDyfx1ErVC7SuivkKqsb2fV
vzC3u+gap6c+rGwrnwgAg9Nakj4y7Z/BWaEy3B6KGkxKY6lnneQ6TKHyOOhMSxby
vzFF5+qFADzWzJLPJ19Yc/UccqR6mQ238vlttX6Em0Xwc3LBNmY64dMzcUqt0FbM
3ry6y2zmdXwURw5yjuv86jCTEfqJ/6ulC2WW/YRTvhBlwl8leQpM8Hq95wSjuypv
MdVaV1QYRHmnTWAtM69Zda3HCnRO+kt0V83p0W5Trec+OXSEzk5tSmCNip9l/Hb+
F3Xwv2gT4KP2r45fL8LheQOelUd+8i6fX0yniluGpjzB+6LpuWNWsFAb3oXrWJVF
wheh2UhzBEg5/YowcFuwn7a1hkT+KbyC6/bC6Syn0ggAkd1EBG8+l8jlsZLX8qVI
xmi7lOgAtHhzdHhAbk5/7KZzYLQAOEd5KH9cgxyqpJu/eRpComRJHLer0wUhqsek
9vxlIz4tkTAmm4ussgePkdKOFwv1UZEBrrP0ApyqDTDKOQwPSLII1XcLT2k5dp+5
/1m53Tlol6eEqr7K6h7EH0kD4wDwPgCxY2VaCRXP+AI2IwRsSjCV5NnRjoKx2vig
IymDIbXTpVu/agvOpRUjNhRhDG+o/iAkDCF4Q3X+LXJygNONlpqr0ZSU8or0tabm
doKWoiTQ23HP4k+BuRVixcTnsj2lFI8VE2ptTxZMIa8wbaoDbeXVtBDnKbb2BEUp
WbQwVGVzdC1Db3JyZWN0IFNlY3VyaXR5IDxzZWN1cml0eUB0ZXN0LWNvcnJlY3Qu
bmw+iJAEExEIADgWIQQjagdL2LTrpwBmhTBsSFw0SpaFXAUCZWXIjgIbAwULCQgH
AgYVCgkICwIEFgIDAQIeAQIXgAAKCRBsSFw0SpaFXILXAP9zKGA5+FyZXtdd+4xr
R7JXJu+DSSTgwS1Gvt2LarGfWgD/R8q20r5WFq8yyblbwo7u+JvHQqSv7hwT2MTe
XS8Dm5+5Ag0EZWXIjhAIALIVK0ObmgorzgH9htPbQR3AijQMgfnpYD5e62b7BRjJ
hjax7LgLn0Pjdm0ap6/8wJM/KIws7pltsnKNx8LynYTr1XFZrNnXeJ+Lsv3BFQha
3FC9AwBXRQqf5BM1533v0UYbl1uAn2hu35m2k4gvLolgZ3OEtcT79NZvGCJ03aRz
BG2xOKRtDA0NoU3QN3dT6w/A6Y4Jm7r4UxmfT/uYMlDb1PwkZF5AAidXcqJ13C42
5m3hYqFt24r09xgLMrPOKiNLndQsHTnIrettSXYirnmKB1zUUN+JKuNCEF4bZy6X
4K9tcw38NOz32eRcST4bLcGBmv9V39aeGG4p7+SshesAAwUIAJaO2dvG3Btd6p3c
lXcAdHHTwXOxERmOLWC5VUr0DQXeEpb4PHn7U7EPNNontZwvvlL3asttJTnC+xbA
dl/UNHStng+ejGLW2B0bCKuR++NTutb0bP5dWNKxlK9c14q7d0izaeuwGlhoJOqC
mR6qXplAOMufl/d0DDeJ2qkzjh51or2Baid48mi9PXGIQQAgBRC0QV3iJ5HfCSgP
u6Us3BeppAzRhFHY1347MMqohuMIDkRyh1sUCkoXBANzobG/oZ7PDgHiZPfCIGUu
sL6vaBZ/bRTFhVjOBGlpJMx4qtLb30AmBTPTa8azt/Pfdwp/jwUjQ/IIq23E3eHU
ZGX3QaaIeAQYEQgAIBYhBCNqB0vYtOunAGaFMGxIXDRKloVcBQJlZciOAhsMAAoJ
EGxIXDRKloVcm+oBAKqrizGE+/7KSKQHb1M4/iwWE20VbqMG2ktozuQRjed9AQCO
ViJEe3xvIxn7PhMWiJwnRLVk4CL0TAb18w5UuQFEiw==
=FoTw
-----END PGP PUBLIC KEY BLOCK-----