Responsible disclosure

Responsible disclosure procedure ICT NML (Nederlands)
ICT NML en haar klanten hechten een groot belang aan de veiligheid van de ICT-infrastructuur en de diverse informatiesystemen. Ondanks dat wij ons best doen om onze systemen zo goed mogelijk te beveiligen, realiseren wij ons dat geen enkel systeem 100% veilig is en dat door menselijk handelen en/of onvolkomenheden in software, kwetsbaarheden kunnen ontstaan.
Wanneer een kwetsbaarheid in ons systeem wordt ontdekt, dan vernemen wij dat graag. We ondernemen dan stappen om de kwetsbaarheid te verhelpen. Door melding te maken van een kwetsbaarheid, verklaart u akkoord te zijn met onderstaande afspraken en zal ICT NML uw melding conform onderstaande afspraken behandelen.

Wij vragen van u:

1. Mail uw bevindingen naar security@ictnml.nl.
2. Geef voldoende informatie om de kwetsbaarheid te kunnen reproduceren, zodat we deze zo snel mogelijk kunnen testen. Meestal zal een IP-adres of URL van het kwetsbare systeem voldoende zijn maar bij complexe kwetsbaarheden kan meer informatie benodigd zijn.
3. Indien u tips heeft om de kwetsbaarheid op te lossen dan stellen wij die uiteraard op prijs. Beperkt u zich hierbij vooral tot de feitelijkheden die rechtstreeks betrekking hebben op de kwetsbaarheid.
4. Laat uw contactgegevens achter om eventueel nadere informatie op te kunnen vragen en/of samen te kunnen werken om tot een veilige oplossing te komen. Laat minimaal een email adres of telefoonnummer achter.
5. Dien de melding zo snel als redelijkerwijs mogelijk in na ontdekking van de kwetsbaarheid.

Het volgende is uitdrukkelijk niet toegestaan:

1. Het plaatsen van malware op onze systemen of die van derden.
2. Via “brute force” toegang te verkrijgen tot systemen, tenzij dit strikt noodzakelijk is om aan te tonen dat de beveiliging van het systeem hier ernstig tekortschiet. Hiermee bedoelen we dat het buitengewoon eenvoudig is om met openbaar verkrijgbare en/of betaalbare hardware en software een wachtwoord te kraken en zodoende het systeem binnen te dringen.
3. Het gebruik maken van social engineering, tenzij om aan te tonen dat medewerkers met toegang tot gevoelige gegevens ernstig tekort schieten in hun plicht om daarmee zorgvuldig om te gaan. Dat wil zeggen als het op overigens volkomen legale wijze (dus niet via chantage of iets dergelijks) in het algemeen te eenvoudig is om hen over te halen tot het verstrekken van dergelijke gegevens aan onbevoegden. U dient daarbij alle zorg te betrachten die redelijkerwijs van u verwacht kan worden om de betreffende medewerkers zelf niet te schaden. Uw bevindingen dienen uitsluitend te zijn gericht op het aantonen van kennelijke gebreken in de procedures en werkwijze binnen ICT NML en niet op het schaden van individuele personen die bij ICT NML werkzaam zijn.
4. Het openbaar maken of derde partijen inlichten over de kwetsbaarheid voordat deze is verholpen.

5. Het verrichten van handelingen die verder gaan dan strikt noodzakelijk om de kwetsbaarheid aan te tonen en te melden. Dit geldt in het bijzonder als u bij het aantonen van de kwetsbaarheid toegang heeft verkregen tot persoonsgegevens of gegevens waarvan u redelijkerwijs had kunnen begrijpen dat deze vertrouwelijk zijn. Een screenshot van een deel van een database is net zo overtuigend als een kopie van de hele database. Het wijzigen of verwijderen van gegevens is *nooit* toegestaan.
6. De beschikbaarheid of bruikbaarheid van een systeem verminderen (denial of service aanvallen, bijvoorbeeld).
7. Op enigerlei wijze misbruik maken van de kwetsbaarheid.

Wat mag u van ons verwachten:

1. Indien u aan alle gestelde voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen u doen en ook geen civielrechtelijke procedure tegen u starten.
2. Als blijkt dat u toch een van bovenstaande voorwaarden heeft geschonden, kunnen wij alsnog besluiten om juridische stappen tegen u te ondernemen.
3. Wij behandelen iedere melding vertrouwelijk en zullen de persoonlijke gegevens van een melder niet delen met derden zonder diens toestemming, tenzij wij daar door de wet of een gerechtelijke uitspraak toe verplicht zijn.
4. Wij delen een ontvangen melding altijd met de Informatiebeveiligingsdienst[2] voor gemeenten (IBD). Zo borgen wij dat gemeenten hun informatie op dit vlak met elkaar delen.
5. In onderling overleg kunnen we u vermelden als ontdekker van de kwetsbaarheid. Dit gebeurt uitsluitend met uw toestemming. In alle andere gevallen blijft u anoniem.
6. Wij sturen u binnen 1 werkdag een (geautomatiseerde) ontvangstbevestiging.
7. Wij reageren binnen 5 werkdagen op een melding met een eerste beoordeling en eventueel een verwachte datum voor een oplossing.
8. Wij lossen de door u gemelde kwetsbaarheid zo spoedig mogelijk op. Daarbij zullen we er naar streven om u zo goed mogelijk op de hoogte te houden van de voortgang en niet langer dan 90 dagen te doen over het oplossen van de kwetsbaarheid. Wij zijn daarbij echter vaak afhankelijk van leveranciers van de door ons gebruikte producten.
9. In onderling overleg kan bepaald worden of en hoe over de gemelde kwetsbaarheid wordt gepubliceerd, echter altijd nadat het probleem is opgelost.

Responsible disclosure procedure ICT NML (English)

ICT NML and its clients consider the security of the IT infrastructure and information systems to be of the utmost importance. Although we do what we can to keep our systems as secure as possible, we realize that no system is 100% secure and that human error and/or imperfections in software can lead to security vulnerabilities.

When a vulnerability in our systems is discovered, we want to hear about it. We will take appropriate measures to mitigate the vulnerability. By reporting a vulnerability, you agree to the conditions outlined below. if you stick to these conditions, we will treat your report accordingly.

We ask of you:

1. To report a vulnerability, send an email with your findings to security@ictnml.nl
2. Supply us with enough information to reproduce your findings. Usually, an IP address or URL will be sufficient but with more complex vulnerabilities, more information may be required.
3. We you appreciate tips you have to mitigate the vulnerability. Please stick to the facts directly related to the vulnerability in question.
4. Provide contact information that we may use to ask you for additional information and/or to collaborate with you to mitigate the vulnerability. At the minimum, provide an email address or phone number.
5. Report your findings as soon as reasonably possible after its discovery.

The following is expressly forbidden:

1. Placing malware on our systems or those of third parties.
2. Gain access by "brute forcing", unless this is absolutely necessary to show that our security is seriously deficient. To clarify: only do this if it is exceedingly simple to gain access using publicly available and/or cheap hardware and software.
3. Using social engineering tricks, unless to show that employees with access to confidential information are exceedingly careless with regards to their duty to safeguard this information. To clarify: this means that it is exceedingly simple to persuade them to provide confidential information to unauthorized individuals using otherwise legal means (so without resorting to threats or blackmail, etc). You should take care not to damage the reputation of the employees in question. Your aim should be to expose the apparent deficiencies in our procedures, not to tarnish our employees.
4. To make the vulnerability public or to disclose the vulnerability to third parties before it is resolved.
5. To perform actions beyond what is strictly necessary to demonstrate and report the vulnerability. Especially if in demonstrating the vulnerability, you have gained access to personal information or information of which you can reasonably be expected to know it is confidential. A screenshot of part of a database is just as convincing as showing us the entire database.
6. To diminish the availability or usability of a system (for instance with a denial of service attack).
7. To take advantage of the vulnerability in any way.

What can you expect from us?

1. If you stick to all the above conditions, we will not take legal action against you or seek to prosecute you.
2. If it turns out that you have violated any of the above conditions, we may decide to take legal action against you.
3. We will treat each report with confidentiality and will not share personal information of the person reporting with third parties without their permission, unless we are required to do so by law or by a ruling of the court.
4. We will share reports we receive with the Informatiebeveiligingsdienst[3] (IBD). This ensures awareness among the community of Dutch municipalities.
5. If you so desire, we can give you credit for the discovery of the vulnerability. We will only do this with your permission. In all other cases, you will remain anonymous.
6. We will send you an (automated) response within 1 work day.
7. We will respond to your report within 5 work days with a primary assessment and if possible, a resolution date.
8. We will mitigate the vulnerability as soon as possible. We will strive to keep you informed of our progress to the best of our ability and not to take longer than 90 days for the mitigation. For mitigations, we may be dependent on the vendors of the products we employ to deliver our services.
9. If all parties concerned agree about the if and how, publication of the vulnerability is permitted but only after the mitigation is in place and the vulnerability is resolved.