Responsible Disclosure Statement (NL) *(ENGLISH BELOW)*

Bij Pathé Thuis vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één 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.

Wij vragen u:

- Uw bevinding toe te sturen via de volgende URL: *https://app.zerocopter.com/nl/rd/bf1d1743-f9af-41c8-88c6-08dfdad4b448.*

Do's:

- Doe een melding zo snel als mogelijk, om te voorkomen dat kwaadwillenden de kwetsbaarheid ook vinden en er misbruik van maken.
- Doe een melding op een vertrouwelijke manier bij de organisatie om te voorkomen dat anderen ook toegang kunnen krijgen tot deze informatie.
- Geef voldoende informatie 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.

Don'ts:

- Onthul de kwetsbaarheid of probleem niet aan anderen totdat het is opgelost.
- Plaats geen eigen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen. Daarmee kan aanvullende schade worden aangericht en onnodige veiligheidsrisico's worden gelopen.
- Misbruik een kwetsbaarheid niet verder dan noodzakelijk is om de kwetsbaarheid vast te stellen.
- Kopieer, wijzig of verwijder geen gegevens van het systeem. Een alternatief hiervoor is het maken van een directory listing van een systeem.
- Breng geen veranderingen aan in het systeem.
- Verkrijg niet herhaaldelijk toegang tot het systeem en deel de toegang niet met anderen.

- Maak geen gebruik van bruteforce attacks, social engineering, aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden om toegang te krijgen tot systemen.

Wat wij beloven:

- Wij reageren binnen 5 dagen 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 of anoniem 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.

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.

Out-of-scope

De volgende merken en daaraan gerelateerde website en apps zijn out-of-scope van ons CVD programma:

- Pathé Nederland (pathe.nl). Wij verwijzen u bij deze door naar het *CVD statement* van Pathé Nederland .

Dit Responsible Disclosure beleid is gebaseerd op een voorbeeld geschreven door Floor Terra en de Leidraad responsible disclosure van het NCSC.

Responsible Disclosure Statement (EN)

At Pathé Thuis the security of our systems is top priority. No matter how much effort we put into system security, there might be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it. We would like to ask you to help us protect our clients and our systems.

Please do the following:

- Submit your findings by using the following URL: *https://app.zerocopter.com/en/rd/bf1d1743-f9af-41c8-88c6-08dfdad4b448*.

Do's:

- Report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it.
- Report in a manner that safeguards the confidentiality of the report so that others do not gain access to the information.
- Provide sufficient information to reproduce the problem, so we will be able to resolve it. 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.

Don'ts:

- Reveal the vulnerability or problem to others until it is resolved.
- Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks.
- Utilise a vulnerability further than necessary to establish its existence.
- Copy, modify or delete data on the system. An alternative for doing so is making a directory listing of the system.
- Make changes to the system.
- Repeatedly gain access to the system or sharing access with others.
- Use brute force attacks, attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties to gain access to the system.

What we promise:

- We will respond to your report within 5 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 concerning the report.
- We will not pass on your personal details to third parties without your permission, unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible.
- We will keep you informed of the progress towards resolving the problem.
- In the public information concerning the reported problem, we will give your name as the discoverer of the problem (unless you desire otherwise).

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Out-of-scope

The following brands and related websites and apps are out-of-scope of our CVD Programme:

- Pathé Netherlands (pathe.nl). Please refer to their *CVD statement* for more information.

This Responsible Disclosure policy is based on an example written by Floor Terra and the Responsible Disclosure Guideline of the NCSC.