

DIVULGATION COORDONNÉE DE VULNÉRABILITÉS PATHÉ HOME (FR)

Date de mise à jour : Mars 2024

Pathé Home accorde une grande importance à la sécurité de ses systèmes, sites Web et applications ainsi qu'à la protection des données à caractère personnel de ses clients, collaborateurs et partenaires. En dépit des moyens déployés et de nos efforts en matière de sécurité, une vulnérabilité jusqu'alors inconnue peut se matérialiser.

Si vous découvrez une vulnérabilité, nous vous prions de nous en informer dès que possible afin de pouvoir prendre des mesures correctives dans les meilleurs délais. Votre aide sera précieuse pour prévenir le risque d'exploitation malveillante.

COMMENT SIGNALER UNE VULNÉRABILITÉ ?

Veillez nous communiquer vos constats sur la plateforme de notre partenaire ZeroCopter en utilisant l'URL suivante : <https://app.zerocopter.com/en/cvd/6ec1dc63-bd9c-4afd-9f0d-0b905c06cbeb>

CE QUE NOUS VOUS DEMANDONS :

- Ne pas exploiter la vulnérabilité plus que nécessaire pour démontrer son existence et notamment en téléchargeant des données pour prouver une fuite, en consultant, supprimant ou modifiant des données, en accédant de manière répétée au système, en apportant des changements au système ou en provoquant un déni de service.
- Ne pas révéler la vulnérabilité à un tiers tant qu'elle n'a pas été résolue.
- Fournir une information suffisante pour reproduire le problème, afin que nous soyons en mesure de le résoudre. En temps normal, l'adresse IP ou l'URL du système affecté et une description de la vulnérabilité suffisent.
- Supprimer sans délai les données confidentielles que vous auriez pu obtenir.

CE QUE NOUS VOUS ASSURONS :

- Nous répondrons à votre signalement dans un délai de 5 jours ouvrables avec notre évaluation.
- Nous n'engagerons aucune action en justice contre vous à propos du signalement dès lors que vous respectez nos conditions.
- Nous traiterons votre signalement de manière confidentielle et ne transmettrons pas vos données à caractère personnel aux tiers sans votre consentement, à moins que ce soit nécessaire pour se conformer à une obligation légale.
- Nous vous tiendrons informé de l'avancée de la résolution du problème.
- Si vous le souhaitez, nous pourrions citer votre nom ou pseudonyme en tant que découvreur du problème dans l'information publique qui serait faite du problème signalé une fois ce dernier résolu.
- Pour vous remercier de votre aide, nous offrons une récompense pour chaque signalement d'une vulnérabilité inconnue.

PÉRIMÈTRE DE CETTE POLITIQUE :

Cette politique s'applique au site Web sur lequel elle est publiée et à l'application mobile et SmartTV correspondantes.

Sites Web de Pathé Home :

- www.pathehome.com
- www.pathe-thuis.nl

Applications de Pathé Home :

- Mobile iOS Application
- Mobile Android Application
- Samsung Smart TV Application
- LG Smart TV Application
- Chromecast
- Airplay

HORS DE PORTÉE :

Les sites Web et applications des autres entités Pathé disposent de leurs propres politiques que nous vous invitons à consulter.

- Pathe.nl
- Pathe.com
- Pathe.fr
- Pathe.be
- Pathe.ch
- Pathe.ci
- Pathe.ma
- Pathe.sn
- Pathe.tn
- Login.Pathe.me
- Pro.Pathe.fr

Cette politique de Responsabilité en cas de Divulgence est basée sur un exemple écrit par Floor Terra et [les lignes directrices concernant la divulgation coordonnée de vulnérabilités du NCSC.](#)

RESPONSIBLE DISCLOSURE STATEMENT PATHE HOME (EN)

Version : March 2024

Pathé Home do care about the security of their systems, websites and applications as well as the protection of the data of their customers, employees and partners. Despite our efforts and means allocated to security, an unforeseen vulnerability can happen.

If you discover a vulnerability, please inform us as soon as possible so that we can take corrective measures without delay. Your help will be valuable in preventing the risk of malicious exploitation.

HOW TO REPORT A VULNERABILITY?

Please send us your findings on our partner's platform ZeroCopter by using the following URL <https://app.zerocopter.com/en/cvd/6ec1dc63-bd9c-4afd-9f0d-0b905c06cbeb>

WHAT WE ASK YOU TO DO:

- Do not exploit the vulnerability more than is necessary to demonstrate its existence, including by downloading data to prove a leak, viewing, deleting or modifying data, repeatedly accessing the system, making changes to the system or causing a denial of service.
- Do not share the vulnerability with others until it is resolved.
- Provide sufficient information to reproduce the problem, so that we can resolve it. Usually, the IP address or URL of the affected system and a description of the vulnerability is sufficient.
- Delete any confidential data you may have obtained without delay.

WHAT WE PROMISE:

- We will respond to your report within 5 business days with our assessment.
- We will not take legal action if you comply with the conditions set by us regarding your finding.
- We will treat your report confidentially and will not share your personal information with third parties without your permission, unless this is necessary to comply with a legal obligation.
- We will keep you informed of the progress towards resolving the problem.
- If you wish, we may cite your name or pseudonym as the discoverer of the problem in public information about the reported problem once it has been resolved.
- As a thank you for your help, we offer a reward for every report of an unknown vulnerability.

SCOPE OF THIS STATEMENT:

This statement applies to the website on which it is published and the corresponding Mobile and SmartTV applications.

Pathé Home websites:

- www.pathehome.com
- www.pathe-thuis.nl

Pathé Home applications:

- iOS Mobile app
- Android mobile app
- Samsung Smart TV app

- LG Smart TV app
- Chromecast
- Airplay

OUT OF SCOPE:

The websites and mobile applications of other Pathé entities have their own statements which we invite you to consult.

- Pathe.nl
- Pathe.com
- Pathe.fr
- Pathe.be
- Pathe.ch
- Pathe.ci
- Pathe.ma
- Pathe.sn
- Pathe.tn
- Login.pathe.me
- Pro.pathe.fr

This Responsible Disclosure Statement is based on an example written by Floor Terra and the [Responsible Disclosure Guideline of the NCSC](#).