Offenlegung

Investment Publishing International BV, der Herausgeber von *Investment Officer*, ist Teil der FD Mediagroep. Die FDMediagroep legt großen Wert auf die Sicherheit ihrer Systeme. Trotz großer Sorgfalt in Bezug auf die Sicherheit der Systeme kann es dennoch Sicherheitslücken geben.

Sollten Sie eine Sicherheitslücke in einem unserer Systeme gefunden haben, bitten wir Sie, uns davon in Kenntnis zu setzen, damit wir so schnell wie möglich Maßnahmen ergreifen können. Wir möchten gerne gemeinsam mit Ihnen daran arbeiten, unsere Kunden und Systeme besser zu schützen.

Bitte beachten Sie: Diese Richtlinie zur verantwortungsvollen Offenlegung gilt nur für Systeme unter Domains, die enden auf:

- `.nl`
- `.be`
- `.lu`
- `.fr`
- `.de`
- `.com`

Andere Domains oder Infrastrukturen liegen außerhalb des Geltungsbereichs dieser Richtlinie.

Wir bitten Sie um das Folgende:

- Melden Sie Ihre Entdeckung per E-Mail an security@investmentofficer.com.
- Nutzen Sie die Schwachstelle nicht aus, z. B. indem Sie mehr Daten herunterladen, als notwendig ist, um das Sicherheitsproblem kenntlich zu machen, oder auf Daten Dritter zugreifen, diese löschen oder verändern.
- Offenbaren Sie die Schwachstelle nicht gegenüber anderen, bevor sie behoben wurde. Löschen Sie vertrauliche Informationen, die Sie während Ihrer Recherche erlangt haben, sofort nach Behebung des Problems.
- Führen Sie keine physischen Sicherheitsangriffe, Social-Engineering-Angriffe, Distributed-Denial-of-Service-Angriffe oder Spam-Angriffe durch und verzichten Sie auf Anwendungen von Drittanbietern.
- Melden Sie uns genügend Informationen, damit das Problem reproduziert und so schnell wie möglich behoben werden kann. Normalerweise reichen die IP-Adresse oder die URL des betroffenen Systems und eine Beschreibung der Schwachstelle aus, aber bei komplexeren Schwachstellen kann mehr erforderlich sein.
- Geben Sie in der E-Mail die CVE-Nummer der Sicherheitslücke an.

Was wir versprechen:

- Wir bestätigen den Eingang Ihres Berichts innerhalb von 5 Tagen.
- Wenn Sie sich an die in dieser Richtlinie genannten Voraussetzungen gehalten haben, werden wir keine rechtlichen Schritte gegen Sie einleiten.
- Wir werden Ihren Bericht vertraulich behandeln und Ihre personenbezogenen Daten nicht ohne Ihre Zustimmung an Dritte weitergeben, es sei denn, dies ist zur Erfüllung rechtlicher Verpflichtungen erforderlich. Eine Meldung unter einem Pseudonym ist möglich.
- Wir werden Sie über die Fortschritte der Behebung auf dem Laufenden halten.
- Wenn wir Sie über das gemeldete Problem informieren, werden wir auf Wunsch Ihren Namen als Entdecker nennen. Als Dank für Ihre Hilfe bieten wir eine Entlohnung für jede Meldung eines uns noch unbekannten Sicherheitsproblems. Die Höhe der Entlohnung richtet sich nach der Schwere der Schwachstelle und der Qualität der Meldung, beträgt jedoch mindestens 50 €. Für die Zahlung benötigen wir eine Rechnung. Wenn es nicht möglich ist, eine Rechnung zu schicken, können wir alternativ einen Geschenkgutschein anbieten.

Wir bemühen uns, alle Probleme so schnell wie möglich zu lösen, und wir sind gerne bereit, uns an der Veröffentlichung des Problems zu beteiligen, nachdem es gelöst wurde.
Die FDMG kann entscheiden, dass für eine potenzielle Schwachstelle mit geringem oder akzeptablem Risiko keine Entlohnung gezahlt wird. Einige Beispiele für Schwachstellen, für die keine Entlohnung gezahlt wird, sind:

- HTTP-404-Codes oder andere Nicht-HTTP-200-Codes;
- Einfügen von Klartext auf 404-Seiten;
- Versionsbekanntgabe bei öffentlichen Diensten;
- öffentlich zugängliche Dateien und Ordner mit nicht sensiblen Informationen;
- Clickjacking auf Seiten ohne Log-in-Funktion;
- Cross-Site Request Forgery (CSRF) auf Formulare, auf die anonym zugegriffen werden kann;
- Fehlen der Kennzeichnung ‚sicher'/‚nur HTTP ' bei nicht sensiblen Cookies;
- Verwendung der Methode HTTP OPTIONS;
- Host Header Injection;
- Fehlen von SPF-, DKIM- und DMARC-Einträgen;
- fehlende DNSSEC;
- fehlende oder falsch angewandte HTTP-Sicherheitsheader wie
    - Strict Transport Security (HSTS);
    - HTTP Public Key Pinning (HPKP);
    - Content Security Policy (CSP);
    - X-Content-Type-Option;
    - X-Frame-Option;

- X-WebKit CSP;
- X-XSS-Protection.