Responsible Disclosure

Investment Publishing International BV, the publisher of Investment Officer, is part of FD Mediagroep. At the FDMediagroep, we consider the security of our systems important. Despite our care for the security of our systems, there may still be a vulnerability

If you have found a weakness in one of our systems, we would like to hear about it so that we can take measures as quickly as possible. We would like to work with you to better protect our customers and our systems.

Please note: This Responsible Disclosure policy applies only to systems under domains ending in:

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

Other domains or infrastructure are outside the scope of this policy.

We ask you:

- Email your findings to security@investmentofficer.com;
- Not to misuse the problem by, for example, downloading more data than necessary to demonstrate the leak or accessing, deleting or modifying third-party data;
- Not to share the problem with others until it is fixed and to delete all confidential data obtained through the leak immediately after fixing the leak;
- Not use physical security attacks, social engineering, distributed denial of service, spam or third-party applications; and
- Provide sufficient information to reproduce the problem so that we can fix it as soon as possible. Usually the IP address or URL of the affected system and a description of the vulnerability is sufficient, but more may be required for more complex vulnerabilities.
- Include the CVE number of the vulnerability in the mail.

What we promise:

- We will respond with a response to the report within 5 days;
- If you have complied with the above conditions, we will not take any legal action against you regarding the report;
- We will treat your report confidentially and will not share your personal data with third parties without your consent unless necessary to comply with a legal obligation. Reporting under a

pseudonym is possible;
- We will keep you informed of the progress in resolving the problem,
- In notifying you of the reported problem, we will, if you wish, include your name as the discoverer; and as thanks for your help, we will offer a reward for each report of a security problem still unknown to us. We will determine the size of the reward based on the severity of the leak and the quality of the report with a minimum of €50. We will need an invoice for payment. If it is not possible to send an invoice, we may look into offering a gift voucher as an alternative.

We aim to resolve all problems as soon as possible and we are happy to be involved in any publication about the problem after it has been resolved. FDMG may decide that a potential vulnerability with low or accepted risk will not be rewarded. Some examples of out-of-scope vulnerabilities include:

- HTTP 404 codes or other non HTTP 200 codes
- Insertion of plain text in 404 pages
- Version banners on public services
- Publicly accessible files and folders containing non-sensitive information
- Clickjacking on pages without a login function
- Cross-site request forgery (CSRF) on forms that can be accessed anonymously
- Absence of 'secure'/'HTTP Only' flags on non-sensitive cookies
- Use of the HTTP OPTIONS Method
- Host Header Injection
- Absence of SPF, DKIM and DMARC records
- Missing DNSSEC
- Missing or incorrectly applied HTTP Security Headers, such as:
    - 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