Deutsche Börse's Responsible Disclosure Policy

Deutsche Börse AG (hereinafter referred to as "Deutsche Börse" or "We/we") takes the security of our systems and data privacy very seriously in accordance with BSI recommendation of using security.txt (RFC9116). We would like to thank all security researchers or members of the public (hereinafter referred to as "You/you") who discover a security vulnerability in our systems and responsibly share the details with us. We appreciate their contribution and work closely with them to address any reported issue with urgency.

Process to report an issue

If you discover a security vulnerability in Deutsche Börse's systems or platforms, we encourage you to report it to us promptly. Please follow these steps to report a vulnerability:

- Contact us: send an e-mail to vulnerabilitydisclosure@deutsche-boerse.com with a detailed description of the vulnerability as described below.

A vulnerability description should have the following information:

- The name of the manufacturer/product owner and whether contact was set up with them.
- The name of the application and the tested version number where applicable.
- A stepwise description (add screenshots wherever possible or other illustrations for better comprehensibility) showing how the vulnerability was discovered (including any tools used).
- An assignment of the vulnerability to the OWASP Top 10 (see https://owasp.org/www-project-top-ten), CWE or CVE. If none of the vulnerability categories fit, this should be described in more detail as "Other".
- Must include proof-of-concept (PoC) in the form of code, screenshots or video along with detailed steps showing how the vulnerability can be exploited.
- An informal declaration if you consent that we include your name/alias of choice in the Deutsche Börse's recognition website (Hall of Fame). Consent can be revoked at any time, and you will be deleted from the recognition website.
- Illustrate your assumed impact of the discovered vulnerability by assigning a severity using CVSS or similar risk rating. Add a description of the impact of the reported vulnerability or a threat model that describes a relevant attack scenario.

You need to adhere to the following terms and guidelines

- No user/customer data shall be modified, deleted, or misused by a security researcher or a member of the public who discovers a security vulnerability.
- Vulnerabilities identified must not be exploited in any form. The foregoing does not limit the possibility of providing a description of the vulnerability as described above and in accordance with the provisions detailed in this policy.
- No manipulation, compromise or modification of systems or data of third parties was carried out.
- Any information and/or finding(s) about vulnerabilities shall be kept confidential between you and Deutsche Börse and not be disclosed to any third party by you. You shall not make your findings publicly available – including via social media, research papers or blogs (personal or otherwise).
- No tools for exploiting vulnerabilities have been offered for a fee or free of charge that third parties could use to commit crimes.
- No attacks (such as social engineering, spam, (distributed) DoS or "brute force" attacks, etc.) were carried out against IT systems or infrastructures.
- Exploiting vulnerabilities for personal gains will lead Deutsche Börse to take strict legal action against you.
- In case of an inadvertent data privacy breach, ensure that you let Deutsche Börse know with immediate effect.
- You will grant Deutsche Börse sufficient time to resolve the issue and close the vulnerabilities identified as indicated in the first response to you.
- Any research conducted shall be in accordance with the laws of the Federal Republic of Germany. You may not violate any applicable laws and regulations, including applicable information technology, data privacy and criminal laws.
- Aid in mitigation of vulnerability, if needed.

You hereby agree to the above-mentioned provisions as detailed under process to report an issue and terms and guidelines. Any deviation therefrom will entitle Deutsche Börse to take appropriate legal action against you.

Scope of the programme

Targets in scope: *.deutsche-boerse.com

Out of scope targets

- All external services/software not managed or controlled by Deutsche Börse are considered out of scope/ineligible for recognition.
- All legal entities of Deutsche Börse Group other than Deutsche Börse AG
- Vendor endpoints
- Delivery endpoints

- 3rd party applications
- Note: link to Out-of-scope targets to be added (Domains and IPs)

Out of Scope vulnerabilities

- Vulnerabilities that do not prove security impact will be considered out of scope for this programme
- Vulnerabilities regarding SPF/DMARC/DKIM records without verifiable proof of spoofing
- Best practice concerns objects like non-session cookies not marked secure and HTTP only, SSL/TLS configuration, missing security headers, etc.
- Vulnerabilities reported by automated tools and scanners without additional proof of concept
- End of life browsers/old browser versions (e.g., Internet Explorer 6)
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Exploits that need physical access to the victim's device
- Host header injection
- Unauthenticated/logout/login CSRF
- Previously known vulnerable libraries without a working Proof of Concept (PoC)
- Any kind of spoofing attack or any attacks that lead to phishing (e.g., e-mail spoofing, capturing login credentials with fake login page)
- Self XSS
- Bugs requiring exceedingly unlikely user interaction, for example social engineering attacks, both against users and Deutsche Börse employees
- Third-party API key disclosures without any impact or which are supposed to be open/public. Specifically, exposed Google Map API keys and keys in Android XML files
- OPTIONS/TRACE HTTP methods enabled
- Known public files or directories disclosure (e.g., robots.txt, CSS/images, etc.)
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Any kind of vulnerabilities that require installation of software like web browser add-ons, etc. in the victim's machine
- Brute force on forms (e.g., Newsletter / Contact us page)
- Missing best practices in Content Security Policy
- Missing SSL, CAA headers
- Functional, UI, and UX bugs and spelling mistakes

Android/IOS – if apps exist

- Exploits that are reproducible only on rooted/jailbroken devices
- Absence of certificate pinning
- Bypassing root/jailbroken detection
- Snapshot/Pasteboard/Clipboard data leakage
- Lack of obfuscation
- Irrelevant activities/intents exported

- Lack of exploit mitigations i.e., PIE, ARC, or Stack Canaries in the IOS app
- Lack of binary protection control

Acknowledgement

We commit, …

- to keep each vulnerability report confidential to the maximum extent permitted by law.
- not to pass on your personal data to third parties without your explicit consent, except where criminal intent was identified or Deutsche Börse is required to do so under applicable law.
- to give feedback on every vulnerability report made.
- not to pursue criminal charges against you if you have complied with the policy and principles as elaborated in this document.
- to be a contact person for a trusting exchange throughout the entire process.

Recognition website (Hall of Fame)

We are currently not part of a cash/bug bounty programme, however, are open to issuing a certificate/recognition website (Hall of Fame) to recognise individuals who report valid security issues responsibly and help us make Deutsche Börse systems more secure.

Changes to this policy

Deutsche Börse reserves the right to change or update this Responsible Disclosure Policy at any time. Any changes will be effective at once upon posting the revised policy on our website.