GoodData Vulnerability Reporting Policy

Last Updated: 11/14/2022

GoodData understands the importance and sensitivity of customer data and recognizes the importance of maintaining an adequate state-of-art information security program. We value and appreciate all reports of potential security vulnerabilities in our platforms and solutions and will take all the necessary steps to review, reproduce, and, where relevant and reasonable, correct the security issues identified by external parties.

- Please report any potential security vulnerabilities to us via security@gooddata.com. When appropriate or necessary due to the nature of the issue, feel free to encrypt your report using our public PGP key.
- Our team will confirm the receipt and forward the report to the Security Operations Team for their review and investigation. Based on the nature of your report, we will get back to you as soon as practicable to validate and confirm the issue.
- If the issue is identified by us as a qualifying issue (as further defined below) and accepted by us, we will schedule a fix in line with our internal patch management practices. We will keep you informed about the progress.
- Please note that any information about the issue while we are working on the fix is considered to be GoodData confidential information and cannot be disclosed unless otherwise approved by GoodData in writing.

Please be aware that you must comply with the legal terms applicable to the specific product or services (see: https://www.gooddata.com/legal/) at all times; particularly, you must not take any actions that might cause an overload, disruption or denial of service of our systems, resulting in an unauthorized access to data belonging to another customer or have a similarly adverse effect on our services or other customers.

Safe Harbor

To encourage responsible disclosures, we will not pursue civil action or file a complaint with law

enforcement for accidental, good faith violations of this policy. We consider activities conducted consistent with this policy to constitute “authorized” conduct under the Computer Fraud and Abuse Act. We will not bring a Digital Millennium Copyright Act claim against you for circumventing the technological measures we have used to protect our products or services in scope if you do so consistent with this policy.

Please understand that if your security research involves the networks, systems, information, applications, products, or services of a third party (which is not us), we cannot bind that third party, and they may pursue legal action or law enforcement notice. We cannot and do not authorize security research in the name of other entities, and cannot in any way offer to defend, indemnify, or otherwise protect you from any third party action based on your actions.

You are expected, as always, to comply with all laws applicable to you, and not to disrupt or compromise any data beyond what this policy permits.

That said, if legal action is initiated by a third party, including law enforcement, against you because of your reporting under this policy, and you have sufficiently complied with this policy (i.e. have not made intentional or bad faith violations), we will take steps to make it known that your actions were conducted in compliance with this policy.

Although we consider submitted reports both confidential and potentially privileged documents, and protected from compelled disclosure in most circumstances, please be aware that a court could, despite our objections, order us to share information with a third party.

Please contact us at security@gooddata.com before engaging in conduct that may be inconsistent with or unaddressed by this policy. We reserve the sole right to make the determination of whether a violation of this policy is accidental or in good faith, and proactive contact to us before engaging in any action is a significant factor in that decision. If in doubt, ask us first!

Guidance for Reporting

When reporting a potential security vulnerability, please always provide the following information:

- Description of the issue (“what have you observed”);
- Potential impact of the issue (“what is the risk to GoodData or our customers”);
- Detailed reproduction steps (“how can we check that the issue is valid”); and
- Your contact details.

Qualifying and Non-Qualifying Issues

The table below lists the types of vulnerabilities for which we are accepting the reports. Please do not submit any potential issues which are listed as non-qualifying; we will not be following up on such reports. Thank you for your understanding.

Qualifying Issues	Non-Qualifying Issues
• Remote Code Execution • Cross-Site Scripting and Cross-Site Request Forgery • SQL Injection • Server-side Request Forgery • Issues related to Authorization and Authentication • Issues related to Access Control or Data Permissions • Misconfiguration of the application and/or infrastructure resources	• DoS / DDoS type of vulnerabilities • User and/or email enumerations • E-mail configuration issues (including but not limited to SPF/DKIM/DMARC misconfigurations) • Missing or insufficient http security flags / cookie flags • Session timeouts • Any reports from automated scanning tools or portals (including Nmap, Nessus, Qualys, sslabs.com tests, etc.)

Hall of Fame

Even though GoodData does not pay any incentives to the security researchers even for the valid vulnerability reports, we express our gratitude by adding their names, should they agree to that, to our Hall of Fame.

We would like to recognize the following professionals for their valuable contributions to GoodData security:

2017

- Stanko Jankovic

2020

- Robin Joseph

2021

- VISA Security team

- Robin Joseph

2022

- Deepak Kumar
- VISA Security Team