JCB Vulnerability Disclosure Policy

1. Introduction

1.1 The purpose of this policy is to set out the rules for Responsible Disclosure to JCB. JCB want to work positively with the security research community to improve our online security.

1.2 JCB supports and appreciates the work done by ethical security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify reproduce and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process and encourage anyone who has discovered a potential security vulnerability in a JCB Information system or service to disclose it to us in a responsible manner.

1.3 Following the receipt of a reported vulnerability, JCB will work to validate and respond to it in a timely manner. We are committed to thoroughly investigating and resolving security issues in our platforms and services in collaboration with the security community.

2. Compliance

2.1 This document applies to any third parties who are reporting vulnerabilities to JCB.

2.2 Third parties are defined as any person or entity who is not employed by JCB or is not directly contracted by JCB to provide a service.

2.3 JCB will carry out their own programme of vulnerability and penetration testing, as outlined in the JCB Information Security Policy and related Information Security Framework.

2.4 Anyone reporting vulnerabilities to JCB must read this document in full prior to reporting any vulnerabilities to ensure that the requirements are fully understood, and any disclosures meet those requirements.

2.5 JCB will publish the security.txt document on JCB web-site under the /.well-known/ path. See Appendix A

3. Responsibilities of third parties

3.1 We do not encourage anyone to actively hunt for vulnerabilities. Vulnerabilities which have been discovered while accessing our information systems can be tested, within reason, to determine the scope of the vulnerability.

3.2 Vulnerabilities may only be tested against an account which the person testing owns or where they have been given express permission by the account owner.

3.3 Any vulnerabilities found must be reported as per the instructions in this policy.

3.4 We expect that any person carrying out vulnerability testing and research will:

3.4.1 Make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our services

3.4.2 Give us a reasonable time to correct the issue before making any information public.

3.4.3 Securely delete all data retrieved during research as soon as it is no longer required and at most, one month after the vulnerability is resolved, whichever occurs soonest.

3.5 We expect that any person carrying out vulnerability testing and research will NOT:

3.5.1 Access or modify (or attempt to access or modify) any data that does not belong to the person carrying out the testing.

3.5.2 Publicly disclose the details of vulnerabilities found without the express written consent of JCB.

3.5.3 Access or attempt to access any data which does not belong to the person carrying out the testing

3.5.4 Send or attempting to send, unsolicited mail, spam or other forms of unsolicited messages.

3.5.5 Upload, transmit, post, link to, send, or store malware, viruses, Trojans or similar harmful software.

3.5.6 Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities (such as an enumeration or direct object reference vulnerability)

3.5.7 Violate the privacy of JCB users, staff, contractors, customers and partners. For example, by sharing, redistributing and/or not properly securing any data retrieved from our systems or services.

4. Out of scope

4.1 Only vulnerabilities which are original and previously unreported and not already discovered by internal procedures are in scope.

4.2 There are also certain activities and vulnerabilities which are out of scope:

4.2.1 Denial of Service (Dos/DDoS) vulnerability attacks.

4.2.2 Volumetric vulnerabilities (i.e. simply overwhelming our service with a high volume of requests is not in scope).

4.2.3 Findings derived by inserting malware of any kind.

4.2.4 Findings derived from social engineering, e.g. Phishing, etc.

4.2.5 TLS configuration weaknesses (e.g. "weak" cipher suite support, TLS1.0 support etc.)

4.2.6 Benign user interface bugs and spelling mistakes.

4.2.7 Any services hosted by Third Party providers are excluded from scope.

4.3 Findings derived from physical testing through methods such as office access (e.g. breaching physical barriers and controls, open doors, tailgating, etc.) may be included in reports but will be passed to the JCB Security Team to investigate.

4.4 JCB will not accept research or security reports conducted by individuals on sanctions lists, or individuals in countries which are on sanctions lists.

5. Reporting Process

5.1 The details of any suspected vulnerabilities should be sent to the JCB Information Security team by sending an email to security-report@jcb.com

5.2 While reporting any suspected vulnerabilities the following information should be included:

5.2.1 Name of the person carrying out the research and testing

5.2.2 Contact details and email address

5.2.3 Summary of the vulnerability its exploit, and potential impact

5.2.4 The testing environment (browser product and version, operating system, mobile app platform, app version, device model).

5.2.5 What product/system is affected (including IP address and URL)

5.3 It is not required to provide a name and contact details to report a vulnerability but without these details we may not be able to investigate further or send any further information that the vulnerability has been verified and resolved. We will only use these details for the purposes of contacting the reporter as part of our investigating and reporting the specific issues you raised. We will ask your permission before sending data to a third party (such as a vendor).

5.4 Details which would allow reproduction of the issue should not be included in the initial report. Details, such as how the vulnerability is triggered, how it is exploited, the specific impact and how you envision it would be used in an attack scenario, may be requested subsequently, over encrypted communications.

5.5 Any personally identifiable information (PII) or financial information (e.g. credit card data) should not be sent to JCB or otherwise disclosed. If we require this data, detail will be requested subsequently, over encrypted communications.

5.6 Vulnerabilities must not be disclosed to 3rd parties or the public prior to JCB confirming that the vulnerability has been mitigated or rectified.

5.8 The security-report@jcb.com email address is intended ONLY for the purposes of reporting product or service security vulnerabilities. It is not for technical support information on our products or services. All content other than that specific to security vulnerabilities in our products or services will be dropped. For technical and customer support inquiries, please visit www.jcb.com

5.9 JCB will not routinely acknowledge vulnerability reports. The IT Security Team will assess the initial request and if further information is required then the reporter will receive an. email acknowledgement within 7 days. A dedicated contact from the JCB security team will be assigned, who will be the primary contact at JCB.

5.10 The dedicated security contact will provide any necessary instructions for encrypted communications of the more sensitive pertinent details and materials.

5.11 The dedicated security contact will liaise with you whilst they manage the resolution process in coordination with the responsible JCB product team(s).

5.12 The Priority for bug fixes and/or mitigations will be assigned based on the severity of impact and complexity of execution.

5.13 The dedicated security contact will confirm when an incident is resolved and, if necessary, work with the reporter to confirm that the solution covers the vulnerability adequately.

5.14 JCB will offer anyone reporting a vulnerability the opportunity to feed back on the process and relationship as well as the vulnerability resolution. This information will be used in strict confidence to help us improve the way in which we handle reports and/or develop services and resolve vulnerabilities.

5.15 The process may evolve over time and any genuine feedback will be valued to ensure that the process is clear, complete and remains relevant.

6. Legal Requirements

6.1 This document is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law or cause JCB to be in breach of any of its legal obligations, including but not limited to:

6.1.1 The Computer Misuse Act (1990)

6.1.2 The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018

6.1.3 The Copyright, Designs and Patents Act (1988)

6.2 JCB will not seek punitive action, such as suspending or terminating accounts, or legal prosecution, of any security researcher who reports, in good faith and in accordance with this document, any security vulnerability on an in-scope JCB service.

Appendix A

https://jcb.com/.well-known/security.txt

Report: Please report any security vulnerabilities to us via the contact method below, only after reading the Vulnerability Disclosure Document. <<https://www.jcb.com/en-gb/vulnerability-disclosure>>

Encryption: Please do not include any sensitive information in your initial message, we'll provide a secure communication method in our reply to you.

Contact: security-report@jcb.com