JCB Vulnerability Disclosure

We want to work with the security research community to improve our online security.

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.

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 platform and services in collaboration with the security community.

This document applies to everyone, including JCB staff and third-party suppliers.

Your responsibilities

We do not encourage users to actively hunt for vulnerabilities; however, vulnerabilities which have been discovered in the course of accessing our information systems can be tested within reason to determine the scope of the vulnerability. You may only test against an account which you own or have been given express permission by the account owner.

We expect that you will:

- Make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our services
- Give us a reasonable time to correct the issue before making any information public.
- 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.

We expect that you will NOT:

- Access or modify (or attempt to access or modify) data that does not belong to you
- Publicly disclose the details of vulnerabilities found without the express written consent of JCB.
- Accessing or attempting to access data which does not belong to you.
- Sending or attempting to send, unsolicited mail, spam or other forms of unsolicited messages.
- Uploading, transmitting, posting, linking to, sending or storing malware, viruses, Trojans or similar harmful software.
- 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)
- Violate the privacy of JCB users, staff, contractors, systems etc. For example, by sharing, redistributing and/or not properly securing data retrieved from our systems or service.

What is out of scope

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

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

- Denial of Service (Dos/DDoS) vulnerability attacks.
- Volumetric vulnerabilities (i.e. simply overwhelming our service with a high volume of requests is not in scope).
- Findings derived by inserting malware of any kind.
- Findings derived from social engineering, e.g. Phishing, etc.
- Findings derived from physical testing through methods such as office access (e.g. breaching physical barriers and controls, open doors, tailgating, etc.)
- Only domains/subdomains which have a security.txt file in their root (i.e. https://<subdomain.domain.tld>/security.txt) are in scope.

- TLS configuration weaknesses (e.g. "weak" ciphersuite support, TLS1.0 support etc.)
- Benign user interface bugs and spelling mistakes.

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

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

What to do if you want to report a vulnerability:

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

While reporting any suspected vulnerabilities, please include the following information:

- Your name
- Contact details and email address
- Summary of the vulnerability its exploit, and potential impact
- Tell us about your testing environment (browser product and version, operating system, mobile app platform, app version, device model).
- What product/system is affected (including IP address and URL)

It is not required to provide your details in order to report a vulnerability but without these details we may not be able to investigate further or send you information that the vulnerability has been verified and resolved. We will only use these details for the purposes of contacting you 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).

Please avoid including any details which would allow reproduction of the issue at this stage. 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.

Please do not send us or otherwise disclose any personally identifiable information (PII) or financial information (e.g. credit card data). If we require this data, detail will be requested subsequently, over encrypted communications.

Please do not disclose any vulnerabilities to 3rd parties or the public prior to JCB confirming that the vulnerability has been mitigated or rectified.

Please read this document fully prior to reporting any vulnerabilities to ensure that you understand the requirements and can act in compliance with it.

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

What to expect

In response to your initial email to security.report @jcb.com you will receive an email acknowledgement, to reassure you that it has been received by us within 7 days.

You will then be assigned a dedicated contact from the JCB security team who will be your primary contact at JCB.

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

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

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

Your dedicated security contact will notify you when the vulnerability is resolved and will ask you to confirm that the solution covers the vulnerability adequately. We will offer you the opportunity to feed back on the process and relationship as well as the vulnerability resolution. This information will be used in strict confidence in order to help us improve the way in which we handle reports and/or develop services and resolve vulnerabilities.

Rewards

Unfortunately, JCB does not compensate individuals or organisations for identifying potential or confirmed vulnerabilities.

Legal Disclaimer

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:

- The Computer Misuse Act (1990)
- The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018
- The Copyright, Designs and Patents Act (1988)

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.

Assistance and Feedback

If you are unsure at any stage whether the actions you are thinking of taking are acceptable, please contact our security team for guidance (please do not include any sensitive information in the initial communications): it.security @jcb.com

This document will evolve over time and your input will be valued to ensure that it is clear, complete and remains relevant. If you wish to provide feedback or suggestions regarding this document, please contact our security team.