Security Vulnerability Disclosure Policy

At Choco we are committed to ensuring the security and privacy of our users. But threats are plenty and issues may still arise.

We genuinely value the assistance of security researchers in keeping our systems secure.

If you believe you've found a security vulnerability in our applications or infrastructure, please reach out to security@choco.com.

This policy outlines the terms that should be followed in relation to vulnerability discovery and reporting.

Scope

All parts of our platform, our Android and iOS application, web app, website (https://choco.com/), software in any form, user interfaces, source code, specifications, IT infrastructure and systems (altogether "Platform") fall under the scope of this policy and are open for security vulnerability discovery.

If you're not sure whether a software is in scope or not, contact us at before starting your research.

Out of Scope

Any software or systems that are not expressly listed above are excluded from the scope of this policy and are not authorized for vulnerability discovery.

Third party applications, websites or services are out-of-scope of this policy even if they may interface or link with our Platform. We are not responsible for consequences you may incur as a result of conducting research on third party owned systems, software or applications.

Reporting

If you find a security vulnerability on our Platform, please report it to as soon as possible. In order to help us solve the problem, add a detailed description of the vulnerability in your report, including:

- Location of the vulnerability (such as URL or screenshot of the exact screen),
- Vulnerability type,
- Potential impact of the vulnerability,
- Steps to reproduce the vulnerability, relevant screenshots, proof of concept scripts or any other

descriptions necessary to reproduce the vulnerability.

To the best of our ability, we will acknowledge the receipt of your report as soon as possible and communicate to you whether we confirm the existence of the vulnerability or not, and if and how we plan to solve it. We will also communicate to you if the vulnerability cannot be reproduced or if it's already been reported.

We will define the validity and severity of the vulnerability based on the impact and the ease of exploitation and determine the actions that will be taken in accordance with our commitment to security and privacy. We'll try to be as transparent as possible about the process and will do our best to notify you when the issue is fixed.

We may ask for your cooperation if additional information regarding the reported vulnerability is required.

Please be aware that Choco does not offer any payments for reporting vulnerabilities.

Guidelines

Security researches should adhere to the following guidelines:

- Do not perform actions which may harm, disrupt, cause interruptions or otherwise impact the Platform, Choco or its users, such as introducing viruses, trojan horses, worms or any other malicious code.
- Do not execute or attempt to execute network denial of service (DoS or DDoS) tests or other tests that may impair access to, interrupt or degrade our Platform, products or place disproportionate load on our infrastructure.
- Do not engage in physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.
- Do not breach security and authentication measures in place.
- Do not access, use or exploit any information except for discovering or reporting security vulnerabilities. You must delete any information you obtained during your research after reporting the vulnerability to Choco.
- Avoid privacy violations and stop your research and notify us immediately if you access any personal data. You must delete such data after notification.
- Do not destroy, corrupt, manipulate, store Choco data or render Choco data inaccessible.
- Do not disclose non-public information of Choco or its users you obtained through your research.
- Do not disclose the security vulnerability until we notify you that the issue is resolved.
- Do not exploit a vulnerability any more than necessary to confirm its presence.
- Do not use an exploit to compromise or exfiltrate data, establish command line access and/or

persistence, or use the exploit to pivot to other systems.

- Do not violate applicable laws, and rights and interests of Choco, its users or third parties.

Intellectual Property

By reporting a security vulnerability, you agree that we may use your reports or any other feedback you provided to update and/or improve our Platform, products and services. You grant us a perpetual, worldwide, royalty-free, irrevocable and exclusive license to use, distribue, reproduce, modify, display, create derivative works and utilize the reports or any other feedback you provided for any purpose at our sole discretion without any further obligations or notices to you.

You represent that your report is your own work and it does not violate the intellectual property rights of any third party.

Legal

By conducting a vulnerability research on Choco's Platform, you agree to be bound by this policy.

We reserve the right to take legal action against security researchers who do not comply with this policy.

We reserve the right to change or modify the terms of this policy at any time without prior notice.