Vulnerability Disclosure Policy

01/24/2024

Introduction

Our purpose is to refresh the world and make a difference, and we can't do that without trust. Central to maintaining this trust is the protection of the information that we've been entrusted with by consumers, our customers and partners, and investors. This policy outlines considerations and commitments for the disclosure of potential security vulnerabilities to The Coca-Cola Company in a responsible manner.

Security Researchers

The Coca-Cola Company recognizes the positive contributions of security researchers and encourages the responsible and direct disclosure of potential security vulnerabilities to us. We accept vulnerability reports from all sources.

Our Commitments to Researchers

- We will maintain standard confidentiality in our communications with you.
- We will work with you to validate and respond to your disclosure.
- We will investigate and use all reasonable efforts to remediate validated issues in a manner consistent with protecting the safety and security of those potentially affected by a reported vulnerability.
- The Coca-Cola Company reserves all of its legal rights in the event of noncompliance with this Policy, but it does not intend to pursue legal action against any party that conducts security research and discloses information to us in good faith and as outlined in this Policy.

What We Ask of Researchers

- We request that you communicate information about potential security vulnerabilities in a responsible manner. This means complying with all applicable laws and the respecting the privacy of individuals. Your security research should also avoid degradation of our user's experiences, disruption to systems, and destruction of data.
- We request that researchers provide sufficient technical detail and background necessary for our team to identify and validate reported issues, using the link below.
- We request that researchers act for the common good, protecting user privacy and security by refraining from publicly disclosing vulnerabilities.

Scope

The Coca-Cola Company defines a security vulnerability as an unintended weakness or exposure that could be used to compromise the integrity, availability, or confidentiality of our digital assets. This policy applies to all digital assets owned, operated, or maintained by The Coca-Cola Company, including applications, systems, public facing websites, and our products.

While many view our Company as simply "Coca-Cola", The Coca-Cola System operates through multiple local channels including our bottling partners who manufacture, package, merchandise and distribute final branded beverages to our customers and vending partners, who then sell our products to consumers. It is especially important that researchers understand the ownership of digital assets that are the targets of their research because of our close partnerships with other companies who may conduct business using the Coca-Cola brand name but are not within the scope of this policy. No part of this policy should be understood to authorize research on behalf of any third-party to The Coca-Cola Company.

The following activities are explicitly out of scope of this policy.

- Compromising the integrity, availability, or confidentiality of non-public information in the possession of The Coca-Cola Company.

- Failing to immediately delete/destroy sensitive information or personal data you may inadvertently access.
- Publicly disclosing any potential vulnerability without the express written consent of The Coca-Cola Company.
- Intentionally or negligently causing a denial-of-service condition for any user beyond the researcher.
- Exploitation of any vulnerability which sends bulk unsolicited or unauthorized messages (spam).
- Conducting research through social engineering or other deceptive means.
- Conducting research by physically connecting to a network or device within a facility operated by The Coca-Cola Company.
- Conducting research against any food or beverage dispensing device (Freestyle, Purefill, Intelligent Vending, Connected Coolers, etc.).
- Security research performed by employees or contingent staff of The Coca-Cola Company and controlled subsidiaries and entities in which The Coca-Cola Company either owns a majority interest or manages operations. These individuals should report potential security vulnerabilities in line with the Code of Business Conduct or other applicable procedure.

We require researchers to contact us before engaging in research that may be inconsistent with or unaddressed by this policy. If in doubt, ask us before engaging in any specific action you think may go outside the bounds of this policy.

Reporting Potential Security Vulnerabilities

The Coca-Cola Company has partnered with Intigriti, a leading crowdsourced security research platform, for the administration of our Vulnerability Disclosure Program.

If you believe you have discovered a potential security vulnerability in any digital asset owned, operated, or maintained by The Coca-Cola Company or a circumstance that could reasonably impact the security of our Company or our users, we encourage you disclose this to us. You may report potential security vulnerabilities to us using this form, please provide all known information related to the suspected security vulnerability you are reporting.

Upon submission, we will acknowledge receipt of each vulnerability report, conduct a thorough investigation, and then take appropriate action for resolution, if any.

While no type of vulnerability is explicitly out of scope of this policy, researchers are asked to consider the attack scenario and exploitability associated with any potential security vulnerability submitted. Prior to submission, please review Intigriti's Standard Disclosure Terms ('Excluded Submission Types', 'Common "Non-qualifying Submission Types') for examples of submission types with limited information or exploitability. In these cases, we may modify our response to your submission.

Click Here To Report A Vulnerability

Last Revised: 01/24/2024