ABInBev

Vulnerability Responsible Disclosure Notice

Table of Contents

Responsible Disclosure Notice

1. Introduction

Anheuser-Busch InBev ("AB InBev" or "We")) strives to protect its technology assets and the data of its employees, partners, customers and others who use our products and services.
AB InBev is committed to supporting the security research community acting in good faith to help us maintain a high standard for the security and privacy of our users. This includes encouraging responsible vulnerability research and disclosure. This Notice sets out our process to review vulnerability disclosed in good faith by security researchers who have not been retained by AB InBev.

Please read this Notice fully before you conduct research or report a vulnerability.

2. Scope

This Notice limits research only to internet facing systems *.ab-inbev.com. Other systems, platforms and services such as IoT are excluded from the scope and are not authorized for testing.
However, if you find a security risk or any other potential issue in a software, system, platform and service developed by AB InBev that merits testing, please contact us before you conduct your research.
Additionally, vulnerabilities found in non-ABI systems from our vendors fall outside of this Notice's scope and should be reported directly to the vendor. If you aren't sure whether a system or endpoint is in scope or not, please contact us.

3. Ground Rules

- Notify us as soon as possible after you discover a real or potential vulnerability.
- You must not violate any applicable law or regulations, including data privacy laws, and must make every effort to avoid degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's 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.
- We take security issues very seriously and would strongly prefer to remediate vulnerabilities before they become public. Thus, all security researchers will wait until we have fully remediated the vulnerability before disclosing to the public. Please note that nothing in the Notice should be construed to prevent you from disclosing issues to regulators/authorities.
- Do not submit a high volume of low-quality reports. Once you have established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test and notify us immediately.
- Only interact with test accounts you own or with explicit permission from the account holder.

Security researchers must not:

- Test any system other than the systems set forth in the 'Scope' section;
- Engage in physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing;
- Send unsolicited electronic mail to ABI users, including "phishing" messages;

- Execute or attempt to execute “Denial of Service” or “Resource Exhaustion” attacks or introduce malicious software;
- Test in a manner known to degrade the operation of ABI systems; or intentionally impair, disrupt, or disable ABI systems;
- Vulnerability and /or extort AB InBev an/or its employees;
- Test third-party applications, websites, or services that integrate with or link to or from ABI systems;
- Delete, alter, share, retain, or destroy ABI data, or render ABI data inaccessible; or,
- Use an exploit to exfiltrate data, establish command line access, establish a persistent presence on ABI systems, or “pivot” to other ABI systems.
- Perform full red-team penetration testing that involves unauthorized access to our servers

4. Safe Harbor

We do not intend to initiate or pursue legal action against any party that conducts security research and discloses information to us in good faith and in compliance with this Policy and guidance from AB InBev. You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this Notice, we will take steps to make it known that your actions were conducted in compliance with this Notice. If at any time you have concerns or are uncertain whether your security research is consistent with this Notice, please submit a report through one of our official reporting channels before going any further.

5. Reporting a Vulnerability

If you believe you’ve found a security vulnerability, please contact our security team at PSIRT@ab-inbev.com. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us); and
- Explanation of how the attack could be executed in a real-world scenario to compromise user accounts or data

6. Reward

ABInBev does not currently offer a “bug bounty” program. Even though ABInBev extends no offer of compensation/reward, it can, at its discretion, consider non-financial compensation for researchers.