Coordinated Vulnerability Disclosure External Policy

Introduction

Abbott Diabetes care (ADC) is a division of Abbott which makes glucose monitoring equipment and supplies for use by diabetics at home or by medical professionals in hospitals and other care facilities . ADC's goal is to help those with diabetes lead fuller, healthier lives by providing access to breakthrough technology that enables them to better manage their disease.

Abbott Diabetes Care (ADC) is committed to ensuring the security of customer’s information within the LibreView product and other Abbott products against potential vulnerabilities. The threat of cyberattacks to medical devices and other systems is constantly evolving. In response, we have proactively established a coordinated vulnerability disclosure program that is focused on reducing the cybersecurity risks from new and emerging threats, enabling us to continuously improve the security of our products. This policy outlines the guidelines that security reporters should follow to report uncovered vulnerability and how to submit discovered vulnerabilities to ADC.

The policy is specific to LibreView and provides details specific to that product or system, and complements the Abbott Cybersecurity Coordinated Product Disclosure Program at https://www.abbott.com/policies/cybersecurity/cybersecurity-coordinated-product-disclosure.html

Scope

This policy applies to all identified security vulnerabilities within the LibreView product, to include: S3 buckets, API endpoints, the LibreLinkUp mobile application, or other resources tied to the LibreView web application. It is not intended to provide technical support information on our products or for reporting adverse events or product quality complaints - please refer to the LibreView website for instructions on contacting support.

Guidelines for Reporting Vulnerabilities

Vulnerabilities should be reported to ADC immediately upon discovery. If you have identified a security vulnerability that could impact our product or our users, please reach out to us by sending an email to adcsecops@abbott.com.

We ask that you please encrypt your email by utilizing our https://abbottadc-pgpkey-security.s3.amazonaws.com/pgp.pub to ensure secure communications with Abbott.

Please provide the following relevant information in your submission. We ask that you refrain from having sensitive information such as personal identifiable or health data as part of the submission in order to ensure the security or privacy of the users are protected.

- Your contact information (contact names, department name, organization name, tracking numbers, email addresses, phone numbers) so that we can get in touch with you.
- The potential vulnerability, including the product name, version number, and configuration details.
- The potential impact of the vulnerability.
- Steps for reproducing the vulnerability, including tools and exploitation code.
- The date and method of discovering the vulnerability, which will help analyze the legibility of the report.
- If the vulnerability is being actively exploited or is known to others.
- Prior or intent of future notification to any other parties (vulnerability coordinators, regulatory entities, other impacted vendors, etc.) of the vulnerability providing any relevant details (tracking numbers, contact information, etc.).
- Information regarding intent to publicly disclose reported vulnerability information

Responsibilities and Procedures

What we expect from you

- We expect that you do not abuse the reported vulnerability. This can be in the form of downloading more than necessary data to demonstrate a vulnerability. If you have identified a vulnerability, use it only as needed to demonstrate the vulnerability.
- Do not perform security testing on devices actively in use or on those systems that will be utilized for patient care delivery after your investigation.
- Do not test in a manner which could degrade the operation of our products; or intentionally impair, disrupt, or disable our systems.
- Do not post or share any information about a vulnerability to the public until the product security team have researched, responded to and addressed the reported vulnerability and informed customers if needed. Public disclosure will be at the discretion of ADC.

What you can expect from us

Upon receiving the vulnerability report, ADC will:

- Acknowledge receipt by replying to your initial email within 5 business days.
- Determine if the vulnerability is within scope of this policy. If the vulnerability is related to an Abbott product outside of the scope of this policy, ADC will forward the vulnerability to the relevant team as per the Abbott CVD Policy https://www.abbott.com/policies/cybersecurity/cybersecurity-coordinated-product-disclosure.html .
- Review and investigate the reported issue/concern, working with the appropriate internal teams for review and verification.

ADC will provide periodic updates to you on the status of the review and investigation.

ADC will identify and take appropriate action to remediate the issue.

Restrictions

ADC will not consider reporters under the age of 13 due to legal considerations when dealing with minors.

This program is not open to any individual on, or residing in any country on, any U.S. sanctions lists.

Notice

Any information shared with ADC may be used by ADC in any manner, in whole or in part, without any restriction. Furthermore, you agree that sharing information with ADC does not create any rights for you or any obligation for ADC.