NowSecure™

Tidepool mHealth App Manages Diabetes

NowSecure Workstation toolkit speeds security testing of the complex app and will validate safe and secure communications over Bluetooth LE.

About

Tidepool operates as a nonprofit organization dedicated to empowering innovation in diabetes management. Its open-source software integrates with continuous glucose monitoring devices, insulin pumps and other diabetes devices to provide accessible, meaningful and actionable data for people with diabetes. The organization awaits clearance from the U.S. Food and Drug Administration for its Tidepool Loop automated insulin dosing mobile app.

Executive Summary

Chartered with a mission of redefining diabetes, Tidepool developed a mhealth app built on the foundation of the do-it-yourself diabetes community's original Loop app that manages insulin dosing. Pending clearance by the U.S. Food and Drug Administration, the app communicates with medical IoT devices via Bluetooth Low Energy (LE) wireless traffic.

Given the complexity of the app and the sensitivity of medical data, Tidepool must ensure the app complies with regulations such as HIPAA and meets the highest standards for security and privacy. The organization uses the NowSecure Workstation automated pen testing toolkit to achieve the following benefits:

- Protect patients from potentially life-threatening cyberattacks
- Speed testing from weeks to a single day
- Gain consistency and repeatability
- Comply with strict regulatory requirements

"NowSecure Workstation enables me to provide fast assessments to my team on a number of key mobile app security features."
— Ben Derr, Security Engineer, Tidepool

The Story

Dedicated to a mission of improving outcomes for people with diabetes, Tidepool developed a new iOS automated insulin dosing mobile app which is currently under review by the U.S. Food and Drug Administration. Tidepool uses the NowSecure Workstation automated mobile application pen testing toolkit to ensure the highly complex mobile app safeguards sensitive medical information, operates in a secure and reliable fashion to maintain patient safety, and complies with strict regulatory requirements such as those mandated by the FDA and HIPAA.

Built on an open-source software foundation, the innovative Tidepool Loop mhealth app integrates with insulin pumps and continuous glucose monitors to help manage blood glucose. Communicating wirelessly over Bluetooth Low Energy (LE), Tidepool Loop examines data on users' insulin, glucose and entered carbs, as well as trending data, and adjusts basal rates as often as every five minutes to reduce or prevent high and low blood glucose levels.

Enhancing Efficiency

Tidepool Security Engineer Ben Derr recognized the high-risk nature of the Tidepool Loop app and the need to thoroughly assess it for security and privacy vulnerabilities that could lead to unwanted data exposure. He recommended implementing NowSecure Workstation based on his experience with a previous employer. Derr continues to rely on NowSecure Workstation to speed testing of the Tidepool Loop mobile app for security, privacy and compliance vulnerabilities and ease remediation.

NowSecure Workstation dramatically increases Derr's efficiency by replacing lengthy manual mobile penetration testing with automated mobile application security testing. Instead of taking about two weeks, he can now deeply examine a mobile app in a few hours using an interactive, wizard-driven interface. "NowSecure Workstation enables me to provide fast assessments to my team on a number of key security features," he says.

"Anything that multiplies my effectiveness so I don't have to spend six hours writing a report delivers huge value."
— *Ben Derr, Security Engineer, Tidepool*

Because he focuses on securing both web and mobile software, Derr lacks the time to spin up a manual test environment or establish a consistent, repeatable testing process that keeps pace with frequent app updates. "There are a lot of great security engineers, but not quite as many great mobile security engineers," he says. "NowSecure Workstation helps bridge those gaps."

Safeguarding Bluetooth

Specific to Tidepool Loop, Derr especially appreciates NowSecure Workstation support for Bluetooth Low Energy (BLE) testing. The Tidepool Loop app will interoperate with diabetes medical devices including insulin pumps and continuous glucose monitors using Bluetooth LE.

The FDA and the U.S. Department of Homeland Security have previously warned the public about potentially life-threatening vulnerabilities in older insulin pumps, pacemakers and other Internet of Things (IoT) medical devices that could allow a cyberattacker to seize control of a device and potentially alter dosages or settings.

Derr worries that an attacker could intercept Bluetooth LE traffic to manipulate traffic between the Tidepool Loop app and connected devices. "Bluetooth testing will be huge for us," he says. NowSecure Workstation examines the pairing between a mobile app and IoT device to determine if Secure Connections and man-in-the-middle flags are enabled for secure authentication.

NowSecure Workstation provides Derr with robust, mature mobile pen testing tooling to deeply inspect mobile apps. "I'm a software junkie and really love using this amazing Swiss Army knife," he says of the kit.

What's more, the user-friendly containerized nature of NowSecure Workstation will enhance the Tidepool QA team's testing of the mobile app as needed. "It's a slickly engineered solution that's seamless to use," Derr says. He likes the tool's advanced testing capabilities for complex apps that feature biometrics, multi-factor authentication and IoT connections.

Simplifying Reporting

Not only does NowSecure Workstation enable Derr to quickly exercise an app, but it greatly eases reporting. Conducting a manual pen test is laborious and security analysts often commiserate about the lengthy process of writing a report to summarize results and cite code examples. NowSecure Workstation essentially eliminates that chore with preformatted, customizable reporting. The reports include contextual data such as CVSS security scores, compliance checks, code snippets, finding descriptions and remediation instructions for developers.

"Anything that multiplies my effectiveness so I don't have to spend six hours writing a report delivers huge value," says Derr. The Tidepool Loop mobile app development team also benefits from such detailed documentation.

Finally, the Tidepool team finds tremendous value in the high level of customer service and support provided by NowSecure. "I know I've got support available if I need it and that's pretty priceless," Derr sums up.