Sloan Smart Faucet Unauthenticated BLE

Medium

← View More Research Advisories

Synopsis

There exists an unauthenticated BLE Interface in Sloan SmartFaucets including Optima EAF, Optima ETF/EBF, BASYS EFX, and Flushometers including SOLIS. The vulnerability allows for unauthenticated kinetic effects and information disclosure on the faucets. It is possible to use the Bluetooth Low Energy (BLE) connectivity to read and write to many BLE characteristics on the device. Some of these control the flow of water, the sensitivity of the sensors, and information about maintenance. Arbitrary BLE characteristics can be read and written commonly via Android/iOS applications (e.g. NRF Connect), Linux command line tools (e.g. gatttool), and more.

Proof of Concept

https://github.com/tenable/poc/blob/master/Sloan%20Smart%20Faucets/sloan_poc.py

Disclosure Timeline

04/01/2021 - Tenable discloses issue to Sloan support
04/16/2021 - Tenable follows up with Sloan support on issue
05/4/2021 - Tenable hears no response from Sloan. Discloses vulnerability details to CERT

Risk Information

CVE ID: CVE-2021-20107
Tenable Advisory ID: TRA-2021-26
Credit: Ben Smith

CVSSv3 Base / Temporal Score: 5.3 / 5.3
CVSSv3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Affected Products: Sloan SmartFaucets including Optima EAF, Optima ETF/EBF, BASYS EFX and Flushometers including SOLIS
Risk Factor: Medium

Advisory Timeline

June 30, 2021 - Initial release

Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media

tenable