

# 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](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

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

*For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.*

*If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)*

## 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

### FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

[→ View all Products](#)

### FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

[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](#)



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

