ADL-1 Security Notice 20250105

Root Cause Analysis

Summary

On Dec 30, 2024 a customer contacted Partisan Labs and reported a defect in the generation of numeric One Time Pads. The defect resulted in the over representation of the digits 1 and 2 in the generated pads.

Root Cause

This defect is in the original firmware from 2017. It occurs in the final step of the numeric pad generation, when the random data is converted to human readable digits for printing.

8k bits of random data is hashed using SHA512 and the resulting value is used as the data for the pad. Each byte of the hash value, was converted to a decimal string using the ‘C’ function itoa which results in a string value between “0” and “255”. This string value was then used as digits for the pad. This is repeated until the total number of digits for the pad has been processed.

The strings “0” – “9” cause no issue, “10” thru “99”, “100”-”199” and “200-255” are the cause of the bias, with the digits 1 and 2 being the worse.

The Fix

The fix for this was to eliminate the integer to string conversion entirely and use mod 10 to obtain a single digit per byte between 0 and 9. This is the same method used to decrypt a OTP encoded message; and the same method, although mod 26, used for the DIANA pads.

This fix has been implemented and is available in version 3.2.1 for ESP based systems and 2.2.0 for Atmel based systems. Update instructions and files are available at

https://partisanlabs.com/adl-1-otp-printer-firmware-downloads/