

ADL-1 Security Notice 20250105

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

We have confirmed this defect does exist and is a software only defect. The underlying TRNG hardware is working properly. The error is in the last stage of pad creation when the random numbers are converted to human readable digits.

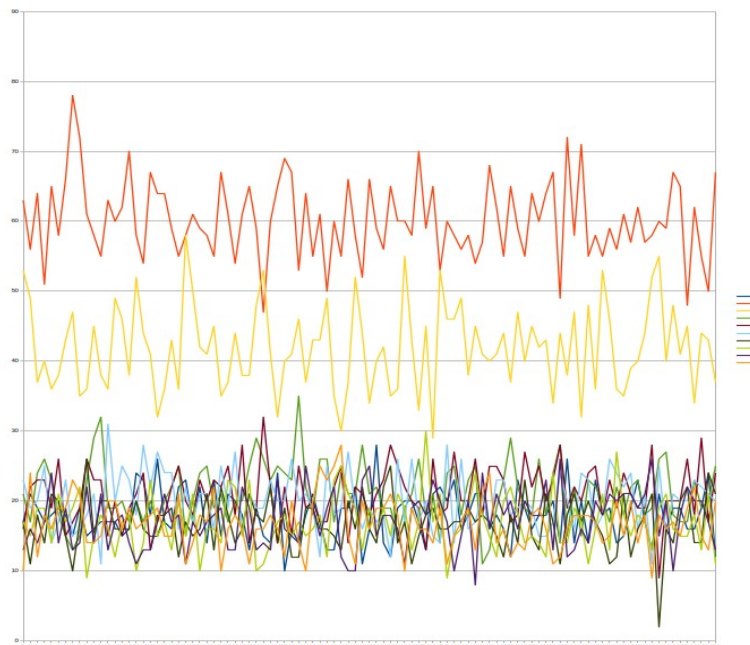
This defect reduces the security of the generated numeric pads to something along the lines of a book cipher. Any numeric pads that have this defect should be used for training purposes only.

The defect has been fixed and an updated firmware package for all version of the printer is available. The new firmware and instructions for updating can be found at

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

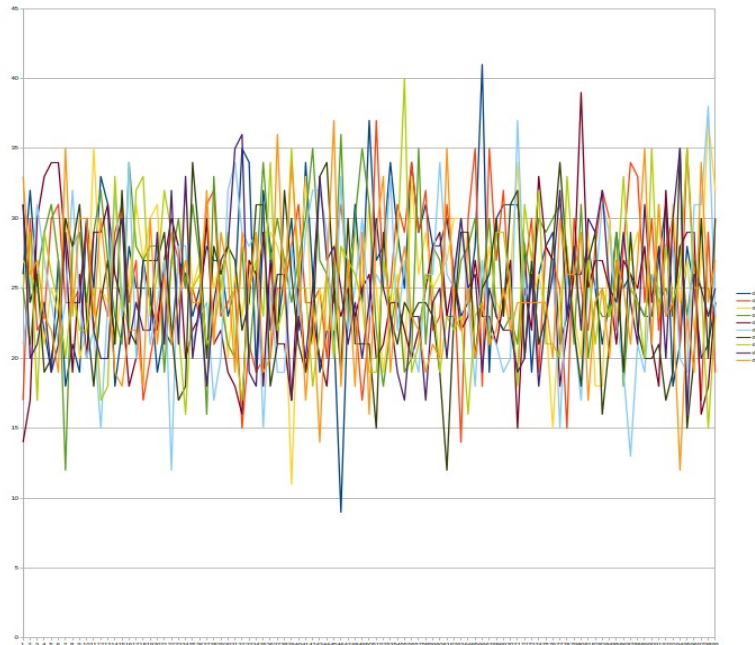
Defect Analysis

Here we can see the effect of the defect over 100 250 digit pads generated in 10 second intervals. Digit 1 in orange and digit 2 in yellow.



Partisan Labs
ADL-1 SCN-20250105

Here is same type of graph with the fixed firmware, 100 250 digit pads, generated in 10 second intervals. Same coloring for the digits.



Significantly better. Full data for 1000 250 digit pads at 10 second intervals along with TRNG Dieharder analysis and Grey scale bitmap analysis are available here

https://partisanlabs.com/wp-content/uploads/2025/01/ADL-1_SN-20250105.zip

SHA512:

a769952dc8bd00950a3749ee19eae04fd0ef2c0dce79ce76dc3ccd56c892a53f6f30ebb0f0f1e22acd28
01dbdd067b05cce5c43248207788b49eaca4b6edec92

TRNG raw and whitened output is available here

https://partisanlabs.com/wp-content/uploads/2025/01/ADL-1_SN20250105_rng-raw.zip

SHA512:

c5b11f2b8062b99d7e830503bc71520e7a825a1ba7f137de934ab6f9916f03d94740c46c5cc249cf9b9
484a88f3045ec107b32601199469d2606e011c915da76

https://partisanlabs.com/wp-content/uploads/2025/01/ADL-1_SN20250105_rng-white.zip

SHA512:

bc5e2aa43f6201357d75cbc6167c2c2410a32f06990305f004f650185c049a5dcd3ff030fc3da7a96638
014e92047022f27cb8829f984a37ccb5950539053888

We apologize for any inconvenience this may have caused you. If you have any questions please email us at support@partisanlabs.com.