CYBERSECURITY ASSURANCE PROGRAM CERTIFICATE

Certificate Number: ULCAP_102
Date of Issue: 2021-03-23
Date of Revision: 2022-05-20
Date of Expiration: 2023-05-20

Certificate Holder: Twilio Inc.
101 Spear St, San Francisco, CA 94105, US

Certified Product: Electric Imp Platform
Model: Imp003, Imp004m, Imp005 and Imp006
Software Version: Imp003, Imp004m, Imp005: impOS version 463e115-release-42.8
Imp006: ImpOS version 203fe10 - release-44.1

Standard: UL 2900-1, First Edition, Revisions through June 5, 2020

NIST Vulnerability Database Date: 2022-05-12

Test Report Number: 4790292670-004

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the UL Global Services Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL trademarks on the Certified Product. UL trademarks may only be used if the Certified Product is also covered under the applicable UL mark program(s).

David Magri

David Magri
Program Manager
Conformity Assessment Programs Office

UL LLC
333 Pfingsten Road
Northbrook, IL, 60062, USA
www.ul.com

Conditions of Certificate

The following conditions must be met for the product to continue to be in compliance with this certificate:

1. The imp003, imp004m, imp005 and imp006 have only been tested as a component. End-product devices and end-product software containing the imp devices were not evaluated.
2. The following version of software included in the product is applicable:
    a. impOS version 463e1157- release-42.8
    b. impOS version 203fe1076 - release-44.1
    c. mbedTLS version 2.6.0
    d. OpenSSL version 1.1.0h
    e. Iwip version 2.1.2
    f. Broadcom WICED SDK version 6.4
    g. Broadcom BCM43907 peripheral drivers version 6.4
    h. ST Micro peripheral drivers version 1.1.0
    i. LZFX compression library version 0.1
    j. Squirrel bytecode interpreter version 3.0.4
    k. newlib version 2.0.0
    l. libgcc version 8.2.0
    m. libgcc version 8.4.0
    n. Monocypher version 2.0.5
    o. Bluekitchen BTstack 51fa0b2
    p. Broadcom Wi-Fi firmware version 5.90.230.35
    q. Broadcom Wi-Fi firmware version 7.45.98.50
    r. Broadcom Wi-Fi firmware version 7.15.168.130
    s. Broadcom Wi-Fi firmware version 7.45.189
3. The implementation of any product specific Cryptographic Module will have to be evaluated as a condition of certification.
4. The implementation of product specific Authentication in the Private Cloud will have to be evaluated as a condition of certification. Electric Imp customers are responsible for their own Certificate Authority and providing key for impOS builds/server images.
5. The implementation of product specific Security Event logging will have to be evaluated as a condition of certification (possibly can be combined with number two).
6. The ability to erase all configuration data, sensitive data and personally identifiable data is product specific and will have to be evaluated as a condition of certification.

7. The implementation of account and privilege management is product specific and will have to be evaluated as a condition of certification.
8. Application code implemented on the device by a product owner will have to be evaluated as a condition of certificate.
9. SSH Bastion host is out of scope for this evaluation.
10. Therefore, if conditions arise where code or protocols implemented by the end product developers introduce risk or bypass security controls; these items would fall outside of the assessment of this certificate.
11. Fuzz testing of the encapsulated communication channel (enabled by an external TLS certificate compromise) has not been performed.