Jump to bottom

Covid Check QRcode Crash App (dos) #146



New issue

○ Closed kfmgang opened this issue on Jul 16, 2021 · 3 comments

Labels

kfmgang commented on Jul 16, 2021 • edited 🕶

Hello.

application will crashes each time the QR code is scanned, the problem is also present on Covid Cert but less problematic, indeed a possible scenario (with a bit of social engineering) is that a person creates a QR code with the payload that crashes the application and presents it to a third party (a restaurant for example), The third party can't check the validity of the certificate because the application will crashes at each scan, the third party could let the access to these services thinking that the certificate is valid and that it's a bug of the application. (Scenario maybe extreme but with a lot of chances that it works).

Only tested on IOS

Payload: { "ver": "1.0.0", "nam": { "fn": "foo", "fnt": "F00", "gn": "bar", "gnt": "BAR" }, "dob": "2000-03-01", "v": [{ "tg": "840539006", "vp": "1119305005", "mp": "EU/1/20/1528", "ma": "ORG-100030215", "dn": 999999999999999999999999999999, "sd": 2, "dt": "2021302-18", "co": "AT", "is": "BMSGPK Austria", "ci": "urn:uvci:01:AT:10807843F94AEE0EE5093FBC254BD813P" }] }

QRcode Payload: Hci:NcF0XNXTSMAHN-HNL458Gi3VRX8S3i0iIC+V 43G-VC9BwH2.W7%\$CML9J77D*QQHIZC4TPIFRMLNKNMBJI0EUG*XNH\$RSC9\$HFE1E0QV1FD/Y4J1ER6W9NT9KP-FHTNP/78LSIT7AZI9\$JAYHIXGGX2M KM16GMJCQ SA KZ*U0I1-10*OCGH0/VNNPM Q5TM8*N9-106H00YQK*R3T3+7A.N88J4R\$F/MAITH-+R2YBV44PZBBAKO1P9-8:0L.A5R8HM*G64TQCV5RQLCUU5WY31-LH/CJ6IAACG423%B04LT HB5Z46/45/G3ZCIATULV:SNS8F-67%21Q21\$4ZW4Z*AKWIX:S:+IZW4PHB033BC786B*E3-433QBV53XEBW77WNN+FNUL]96B4UN*97\$IJV7776B3D3CZK7%2RZ4QWCS46147TMH56ML*H:/E6 N\$YPQ98ZF0HYGKZNZXVB NEHFXHV\$0T2VMF%UVRC-/623WU-F*NF\$:II947HAT6UPDMUIP6 4JXD-5W7GGLZO-TEB403SRF2



Hoping to have helped ^^

goebelUB commented on Jul 19, 2021

Contributor

Thanks a lot for the report.

I can reproduce the crash and the iOS team will look into it.

(which we catch and propagate as a decoding error).



SquebelUB added the bug label on Jul 19, 2021

☐ Stmitt mentioned this issue on Jul 20, 2021

 $\textbf{Remove a fatal error in UnkeyedDecodingContainer} \ \text{eu-digital-green-certificates/SwiftCBOR\#1}$

Merged
 Me

☐ This was referenced on Aug 16, 2021

updates packages admin-ch/CovidCertificate-SDK-iOS#82

Merged
 Me

Update SDK to latest version #163

Merged
 Me

kfmgang commented on Aug 25, 2021

Author

Just to inform you that I can't reproduce the crash on the 2.4.0 👍 @goebelUB

goebelUB commented on Aug 26, 2021

Contributor

Thanks for confirming, and thanks again for reporting this!

Maxelweb mentioned this issue on Jan 1 [DOCS] QR Code Attacks - Literature Maxelweb/FuzzQR#2 Oclosed F) 6 tasks
signees
one assigned
bels .
ug
ojects
ne yet
lestone
milestone
velopment
branches or pull requests

2 participants

