sysmocom

systems for mobile communications GmbH

sysmoEUICC1 security bulletin 2025/07

Revision v3

July 10, 2025

Author: Harald Welte

1 Introduction

As a result of independent security research, vulnerabilities have been found in the Card Operating System (CardOS) used in the sysmoEUICC1-C2G. This CardOS is developed by and licensed from Kigen, one of the major vendor of SIM card operating systems.

Those vulnerabilities are described to permit the sophisticated attacker to extract both the secret key material of mobile operators (K + OP/OPc) from eSIM profiles installed on the card, as well as the secret key material identifying the eUICC itself to the SM-DP+ (eSIM download server).

All our customers of affected products are strongly advised to deploy the mitigation measures described below.

We like to point out that sysmocom as licensee of the CardOS has had no role in the development of it. The responsibility for the security of the CardOS is entirely with our upstream supplier Kigen.

1.1 Affected Products

- **sysmoEUICC1-C2G** with ATR 3B9F96803F87828031E073FE211F574543753130136502
  If the sysmoEUICC1-C2G has been part of a customer-specific order without pre-installed test profile, the initial attack vector used is not exposed. Nevertheless, applying the mitigation patch will add protection in case a TS.48 test profile is loaded at runtime.
- **sysmoEUICC1-CMG** with ATR 3B9F96803F87828031E073FE211F574543753130136502
  This product is affected bt the vulnerability, but does not ship with a pre-installed GSMA TS.48 test profile with known key materials; hence the initial attack vector used is not exposed. Nevertheless, applying the mitigation patch will add protection in case a TS.48 test profile is loaded at runtime.
- **sysmoEUICC1-C2T** with ATR 3B9F96803F87828031E073FE211F574543753130136502
  This product is technically also affected by the vulnerability, but given that is is used with well-known and hence insecure-by-design GSMA SGP.26 keys for the sole purpose of testing, there are no known security implications.

1.2 Unaffected Products

Any sysmoEUICC1 variants with ATR 3B9F96803F87828031E073FE211F574543753130346525. Those are using a later version of the Kigen CardOS that already includes mitigations built-in.

2 Mitigation

Kigen has provided mitigation measures against the vulnerability.

2.1 Patch for existing sysmoEUICC1 in the field

Kigen has provided a patch for the existing sysmoEUICC1. The patch consists of a very short sequence of APDUs that need to be sent to the EUICC. This can be done e.g. by inserting the sysmoEUICC1 in a smart card reader attached to a computer and executing a pySim-shell to perform the patching of the card.

For sysmoEUICC1-C2G/C2M deployed in remote devices in the field, it is recommended to apply the patch from the operating system that controls the cellular modem in the device. All that is neede is e.g. a few AT commands (AT+CSIM) to issue the patch APDUs towards the eUICC.

sysmocom requests customers to **report the specific EIDs to which they were able to apply the patch** to `euicc-security@sysmocom.de`

Failure to apply the patch may potentially result in certain MNOs/MVNOs considering to black-listing unpatched eUICCs (EIDs) at their respective SM-DP+, which in turn would mean that no future eSIM profiles of such operators would be possible to download+install. This is a purely hypothetical danger at this point, and we are not a ware of any MNOs/MVNOs who actually announced any such measures. However, we believe applying the patch as a defensive measure against such an eventuality is in the best interest of our users.

2.2 Updated sysmoEUICC1

Starting end of July, sysmocom will start shipping an updated version of the sysmoEUICC1 products (all variants) based on an updated Kigen CardOS which contains built-in mitigations against the attack.

3 Futher information

- Original Research by Adam Gowdiak of the polish IT security company Security Explorations: https://security-explorations.com/esim-security.html
- Kigen Security Advisory of June 27, 2025 (attached)

4 Contact

If you have questions about how to apply the patch or any other inquirty related to this vulnerability, please reach out **only** to `euicc-security@sysmocom.de`

5 Appendix A: Patch as pySim-shell script

You can find the patch APDUs to be executed using pySim-shell below.

NOTE: The green numbers at the beginning are line numbers to show you which lines are printed as multiple lines here purely due to the constraints of the text processor / document width.

```
 1  reset
 2  apdu 00A4000C02ABCD --expect-sw 9000
 3
 4  apdu
00D60000FF6ECEA8EADF4DAB184543753130313365202503280154008CA434D6A2A832B6F7064130
EB62C94C7535E1E3F038BC614BD9D5451849EECD7740A5C483D8D9D87C544267D554D87FD0C710B7
CB3245DE322BAFBC8BABBB39DB5813633FEC5DA9C68ED3F62A919DAA3AEB5C5E03EB2B530E309FCC
90609E19A98509CF41434BE4A471340694E15DFBD7628986B755F5F9A403B03101713AEB70C58620
8744F812049DB463CDFA5CB6ECF223CEB48A22FD0513E0FDFD8F799AF92C4693583DC53D4E69FFA6
BE914D1FD85036EC67126756A0276CEAF7F2719E55BBC61E32D04746FDA4CA86EF4EFD155EC2C2AC
3A3DA0116B29B5A4B8EFA5CECE7F48D4D53D1C14 --expect-sw 9000
 5
 6  apdu
00D600FFF9469EE37C958FB325C70FDD0E3462905ADBC395B2C5B64A02C15BB9319F394314A80652
0328AA103EE697BC45BC413B84F2BA43B76B0D196CE9CF68035C0E9C173B0DA8B9052F010459CAD2
99EC6280B6D6581B0B88DADB6AA6CFBEE45DFB0FCE8B0BB560CD07F9A32C43071A37B4216D4AB955
A9114DDC76ABAC6A696730C18C7E0853A287A5A14C80C003300E9562D178F1DF5CE9C1FF609B2B74
804287F075F6143C2DF2292C6F406DFF95F1CD9E60A9E0889BAB9BB3CECB2E3DAE69848B6E89F3FF
9BCE92AE4BBEF3C5C5F88C107722ECE70B7BA22E234F8AD5492E4783CB522A68862FAD35B47D6E49
5091F46202A9F5BA6A7F9A6760C5 --expect-sw 9000
 7
 8  echo Check if the patch has been correctly applied...
 9  apdu 00A4000C02ABCE --expect-sw 9000
10  apdu 00D600001D0145437531303133652025032 8CCFD4D39E1F60A7D29B0694957DC8A6C
--expect-sw 9000
11  apdu 00B000001D --expect-sw 9000 --expect-resp
024543753130313365202503280000000000000000000000000000000000
```

27 June 2025

Kigen
c/o Mishcon De Reya
Four Station Square
Cambridge CB1 2GE
United Kingdom

kigen.com

Security Advisory – Action Required for eSIM Vulnerability Patching

Dear Valued Customer,

Kigen is issuing this security advisory to inform you of two recently identified vulnerabilities affecting specific eSIM configurations. We are providing this communication to support your engagement with your end-customers and to assist in appropriate mitigation and patch planning.

While the terms of your existing Non-Disclosure Agreement (NDA) with Kigen may ordinarily limit the scope of communication, Kigen authorises the full content of this letter to be shared with your end-customers and other relevant stakeholders, solely for the purpose of ensuring timely and effective remediation of the identified vulnerabilities. Please note that your customers should continue to follow the existing NDA terms and conditions you would normally have in place with them.

Summary of Security Issues

Kigen has identified and addressed two critical issues:

1. Vulnerability in GSMA TS.48 Generic Test Profile (≤ v6)
Earlier versions of the GSMA TS.48 Generic Test Profile exposed Remote Applet Management (RAM) keys. This exposure undermined the JavaCard chain-of-trust, allowing unauthorised applet installation on the eSIM.

2. Illegal Bytecode Enabling Out-of-Bounds Memory Access
This vulnerability involves a class of illegal bytecode executable only in the absence of proper JavaCard bytecode verification. It allowed unauthorised memory access and was exploitable only when combined with the above RAM key exposure or equivalent chain-of-trust compromise. For further technical context on JavaCard trust models and bytecode verification, we recommend the following resource: https://blogs.oracle.com/javamagazine/post/learn-more-about-java-card-verification-and-deployment-model.

Patch Availability and Mitigation Measures

As of April 2025, Kigen has released security patches across all eSIM Operating System (OS) variants to:

- Enforce GSMA TS.48 Generic Test Profile v7 compliance, preventing applet installation in Test Profile.
- Harden OS internals to block the specific illegal bytecode

Kigen
c/o Mishcon De Reya
Four Station Square
Cambridge CB1 2GE
United Kingdom

kigen.com

classes, thereby preventing any unauthorised memory access.

The patch, approximately 180 bytes in size, mitigates both vulnerabilities and is available for both Consumer (SGP.22) and M2M (SGP.02) OS variants. Patches can be accessed via established distribution channels or by direct request to Kigen.
Prioritisation was based on risk exposure, beginning with customers using GSMA TS.48 Test Profiles. All customers were informed well ahead of anticipated public disclosure.

Customer and End-Customer Communications

Kigen strongly encourages all customers to:

- **Inform their end-customers** of the availability of the patch.
- **Recommend prompt application** of the patch to all potentially affected eSIMs.
- **Reassure** that risk is fully mitigated post-update.

It is important to note that unauthorised applet installation requires a break in the chain-of-trust, which was made possible primarily through the use of GSMA TS.48 v6 or earlier. However, the possibility of alternative compromise paths means **end-customers should consider patching all eSIMs**, regardless of profile version, based on their risk tolerance.

Additionally, **some Mobile Network Operators may require all eSIMs to be patched** in order to allow successful profile downloads. Kigen continues to work closely with network providers to ensure these requirements are clearly communicated and that customers are empowered to make informed decisions balancing security with operational considerations.

Authorised Sharing

This communication, in its entirety or as part of derivative summaries, **may be shared** with your customers and affected parties under the scope of this advisory. Sharing does **not** constitute a breach of your NDA with Kigen.

For further technical assistance or support in preparing end-customer communications, please contact your Kigen account representative.

Kigen (UK) Limited