# admin/1423: On the Insecurity of Open-Source 5G Core Network Deployments in the Wild

Katharina Kohls
*Ruhr University Bochum*
*Bochum, Germany*
*katharina.kohls@rub.de*

***Abstract*—5G promises improved performance and security features for our communication infrastructures, and cloud implementations of 5G core networks make private deployments more accessible. They accelerate the distribution of 5G-based communication networks for various use cases. However, the accessibility of a functional network implementation also bears the risk of maintaining a complex infrastructure with insecure configurations. In this work, we conduct a measurement study that focuses on selected interfaces of exposed core networks on the Internet. To this end, we scan for exposed management interfaces and analyze their security regarding insecure default login credentials, JWT tokens, exposed GTP ports, and cluster APIs. Our results indicate that a high number of deployed networks must be considered insecure.**

***Index Terms*—5G core network, measurement study, gtp security**

## 1. Introduction

As a novel feature, 5G opens up the core network and follows a modular, service-based architecture [1]. In contrast to prior generations that relied on monolithic core network implementations, the 5G core network now overcomes the state of being a black box backbone. With the modular architecture, core network components no longer depend on a single closed implementation, but individual functions can be acquired from different sources. We already experience the benefits of this development in the cloud-based and open-source implementations of 5G core networks that make custom network deployments easily accessible [2], [3]. With standard hardware it is possible to deploy a functioning 5G core network within a matter of hours. These implementations currently serve scientific, private, or commercial projects and are available online [4], [5]. As a result, we can expect an increasing number of 5G core networks in the coming years.

While the availability of open-source core networks significantly contributes to their accessibility, this also bears the risk of running and maintaining a complex and powerful infrastructure with insufficient awareness for its security requirements. One example of this is the use of web-based management interfaces that allow for configuring the network through a simple website, e.g., to register new users. Although this comes as a handy feature, it also creates an important entry point for adversaries, for example, with the goal to register malicious users in the network. In case the management interface is not sufficiently secured, the security of the entire network deployment is harmed: the web portal provides access to the permanent key that functions as the root security measure of all communication in the network.

We find similar dependencies for other interfaces of core networks. For example, virtual network deployments in cluster environments provide a flexible solution that does not depend on dedicated hardware. [6], [7]. Another example is the use of JWT tokens for the assignment of administrator rights. When used with all security precautions in place, such tokens can simplify the authentication and rights management in the core network. However, the use of default credentials enables an adversary to self-assign said access rights with, again, consequences for the overall security of the network [8].

Unfortunately, the current state of the art does not provide empirical results or dedicated measurement tools to document the state of open-source 5G deployments in the wild. Existing work provides geographical measurements on different attack vectors [9]–[11], or uses a crowd-sourced approach to obtain results [12]. Systematic security analyses focus on risk assessment for network implementations [13]–[16] or aspects of general performance [17]–[22]. In contrast to both directions of related work, we focus on the individual characteristics of easily accessible open-source implementations of 5G networks.

As 5G is still in an early stage of its deployment and open-source implementations are in the making, frequent changes in the available security standard occur. Unfortunately, the current state of the art does not provide suitable assessment tools that provide us with empirical results regarding the current state of deployed 5G networks.

In this work, we conduct a measurement study that provides insights on the security of two prominent open-source core network implementations for 5G, namely, Open5GS and free5GC [23], [24]. Our experiments focus on interface-specific security capabilities of network deployments that can be found on the Internet. During a course of 10 months, we perform daily scans of the Internet and document the presence of management applications of two prominent open-source 5G core networks. Our results indicate exposed interfaces that use publicly known default login credentials, and point out exposed GTP services. We further provide results on the use of JWT tokens in these systems and document open Kubernetes and Kubelet APIs in this context. Our results reveal that a significant number of publicly accessible networks use highly insecure configurations. In summary, we make the following contributions.

- We conduct a 10-month measurement study that gathers information about two prominent open-source core network implementations (Open5GS and free5GC).
- We analyze the gathered results and provide insights on the current state of security in publicly accessible deployments. Our results indicate insecure configurations and open interfaces for many of the existing deployments.
- We discuss the implications of our findings and propose measures that can improve the overall security status of open-source deployments.

## 2. Technical Background

A 5G mobile network consists of the end devices (User Equipment, UE), the radio tower (gNodeB), and the core network. The different radio towers are connected to the core network using a GTP tunnel (GPRS tunneling protocol).

**Core Network.** The 5G core network is a software implementation using a service-based architecture that consists of individual functions. A series of open-source solutions provide 5G core network implementations that can be deployed in a virtual environment or on dedicated hardware. In this work, we are particularly interested in selected *interfaces* of open-source core networks. (i) Web-based management interfaces enable configuration options for a deployed network. (ii) The GTP port of the core network makes it possible to connect to the radio components of the network. Furthermore, we analyze (iii) open APIs in virtual deployments and the use of JWT tokens for rights management.

**Management Interface.** Web-based management interfaces provide a subset of network configuration options that can be adjusted through a website. An important part of this is the management of existing and new users, i.e., for entering and changing the credentials of subscribers. Access to these functions is granted through a simple login interface that requires either a username and password, or uses JWT tokens. We focus on three security-relevant characteristics of management interfaces. First, adversarial access to the permanent identities of users involves sensitive subscriber information and introduces privacy implications. Second, the adversary is able to add malicious users to the network. Third, the spoofing of JSON web tokens provides access to the database of the network [25].

**GPRS Tunneling Protocol.** The GPRS Tunneling Protocol (GTP) enables IP connections in mobile networks, as it establishes a tunnel connection between the user equipment and the packet data network. This is achieved by establishing a single fixed endpoint for the IP connection, which can be addressed even when the user moves and connects to different radio towers. In this work, we focus on exposed GTP ports that enable an adversary to connect to the 5G core from an outside network, which provides direct access to core network functions.

## 3. Measurements

We conduct a series of measurements that crawl the Internet for exposed interfaces in open-source core network deployments. In the following, we illustrate our measurement procedure and document the dataset characteristics of our collected results.

TABLE 1. GTP PORTS PER COUNTRY.

| | | Portals | GTP Ports |
|---|---|---|---|
| Measurements | Total | 58 890 | 14 628 |
| | Shodan | 9851 | 14 628 |
| | Censys | 49 039 | - |
| IPs | Total | 642 | 13 495 |
| | Open5GS | 535 | - |
| | free5GC | 109 | - |
| Countries | | 34 | 87 |

### 3.1. Methodology

We focus our measurements on the two prominent open-source implementations free5GC [3] and Open5GS [2].

**Measurement Targets.** Both implementations provide a web-based management interface that, if not adjusted during the installation and setup procedure, can be accessed using default credentials. Furthermore, we document open GTP ports that indicate the presence of a mobile network and, due to the open port, offer a certain attack surface. We further document the use of JWT tokens that make use of default cryptographic credentials and test for open Kubernetes and Kubelet APIs.

**Measurement Tools.** We use Shodan [26] and Censys [27] to scan the Internet for exposed management interfaces and ports. Our search queries focus on the HTTP title of websites that host a management interface. To reduce the number of false positives, we perform a secondary search for substrings within the HTML source of detected candidate sites. We source these substrings from confirmed deployments of management interfaces from both implementations and focus on unique characteristics like a specific logo or a string in the title. We find open GTP ports by searching for endpoints that respond to a GTP echo request.

### 3.2. Dataset Characteristics

Our measurements cover a period of 249 days from May 2023 until January 2024 with the first measurement being conducted on 2023-05-23 and the last on 2024-01-28. An error in the measurement pipeline splits this period into two phases with an outage in August and September 2023. This results in 65 days coverage for the first phase and 104 days coverage for the second phase.

Table 1 provides an overview of the dataset characteristics. Given the two phases of the measurements, we achieve an average of 348 results per day for the search for management portals, and 86 results per day for the GTP portals. In our analysis we combine the results of both search engines whenever possible and ignore duplicate[1] findings for identical timestamps.

1. A duplicate is defined as two findings of the same IP address and implementation, e.g., through the same result obtained by two different search engines.

TABLE 2. AGGREGATED RESULTS FOR BOTH IMPLEMENTATIONS.

| Status | Impl. | Mean | Med | Min | Max |
|---|---|---|---|---|---|
| Exposed | free5GC | 10.4 | 12.0 | 1 | 20 |
| | Open5GS | 52.0 | 48.0 | 28 | 79 |
| Vulnerable | free5GC | 11.0 | 10.0 | 1 | 25 |
| | Open5GS | 36.0 | 36.0 | 21 | 49 |

Within our data set, we observe 642 individual IP addresses. We use the IP address as an indicator for unique endpoints in our results. Out of these individual IP addresses, 535 IPs result from Open5GS instances, and 109 IPs result from free5GC instances.

## 4. Analysis

Our analysis focuses on the potential security threats related to specific interfaces of the core network. First, we analyze the occurrence of publicly available management portals that use the default set of login credentials (Section 4.1). In the same context, we further analyze the presence of open Kubernetes and Kubelet APIs for deployments of Open5GS, and the existence of default JWT secrets for free5GC. Second, we analyze the number of exposed GTP ports (Section 4.2).

### 4.1. Default Login Credentials

Both core network implementations in our experiments provide a web-based management portal that is pre-configured with a default username and password. Regarding the security of the core network deployment, we can derive the following three states:

1) **Vulnerable:** The management portal can be reached from the Internet and uses the default username and password. *Direct access possible.*
2) **Exposed:** The management portal can be reached from the Internet and uses a custom username and/or password. *Access depends on security of username/password. Deployment visible.*
3) **Hidden:** In the hidden state the core network implementation either does not provide a management portal or prevents it from being accessible from the Internet. *No access possible.*

**4.1.1. Daily State.** The daily state of observed endpoints documents the number of unique IP addresses that we found during our regular measurements. More precisely, we analyze all endpoints (including multiple open ports at the same IP address) and denote an IP address as exposed in case we find at least one accessible management portal but no use of the default credentials. We denote an address as vulnerable in case any of the accessible portals makes use of the default username and password.

Figure 1 illustrates the number of endpoints for vulnerable and exposed management portals during both phases of the experiment. The results summarize the findings for both core network implementations and give a first impression of the number of active deployments worldwide.

The results indicate an overall higher number of exposed endpoints in comparison to those that are deployed with the default login credentials. In both cases we observe a slight decline in the total number of endpoints. Table 2 further aggregates the results for both implementations individually. The numbers indicate that Open5GS is the overall more prominent core network implementation with both a higher number of exposed and vulnerable management portals.

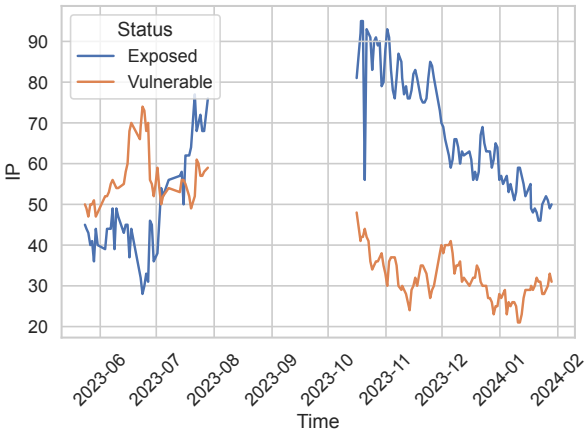


Figure 1. Daily status of exposed and vulnerable endpoints in the combined measurement results of both core network implementations and search engines.

TABLE 3. AVERAGE STATUS CHANGES IN ENDPOINTS.

| Impl. | free5GC | | Open5GS | |
|---|---|---|---|---|
| Port | Other | SSH | Other | SSH |
| Status Changes | 10.1 | 0.0 | 4.3 | 0.0 |
| Days Exposed | 156.3 | 17.5 | 33.3 | 32.0 |
| Days Vulnerable | 8.8 | 0.0 | 13.5 | 0.0 |
| To Exposed | 5.1 | 0.0 | 2.4 | 0.0 |
| To Vulnerable | 5.0 | 0.0 | 1.9 | 0.0 |

**4.1.2. Status Changes.** We are further interested in the persistency of the observed endpoints. To this end, we distinguish the two network implementations and analyze their uptime regarding status changes and the number of days within a certain status. Table 3 summarizes the average behavior observed in the obtained data set. The status changes indicate a change from one status to another, e.g., in case an endpoint first occurs as exposed and later appears to be vulnerable (or the other way round).

In the analysis of status changes we point out a specific technical characteristic that allows us to distinguish the results further. Depending on the observed port we are able to analyze instances that can be accessed through SSH (Port SSH) or those that are general web instances of management portals (Port Other). All SSH endpoints introduce another security status for the system, i.e., they indicate the possibility to access the core network implementation via SSH. Please note that we did not attempt to follow through on the SSH access.

Our results indicate that for both implementations a low number of status changes occur. However, these changes happen in both directions leading to deployments that seem to become vulnerable over time. Furthermore, the analysis is in line with the previous documentation of the daily status: the majority of endpoints exposes

the management portal without using the default login credentials, hence the significantly higher number of days in the exposed status rather than the vulnerable status.

**4.1.3. Open APIs.** In the broader context of privilege escalation within 5G core networks, we analyze two further characteristics including the handling of JWT tokens within Open5GS and the number of free5GC deployments that use an open API to underlying Kubernetes and Kubelet clusters.

**Open5GS: JWT Token.** A server can generate a JWT token to assign a certain claim to a user. In the context of the Open5GS implementation such tokens are used to assign administrator rights. JWT tokens are signed and use optional encryption to protect said claims. However, the specific implementation that can be found in Open5GS uses the default secret key to craft a token. This default credential is publicly available and, eventually, allows an adversary to craft a valid token that grants administrator rights in the network without an expiration date.

In our measurements we test for the use of default secrets in the JWT tokens as an indicator for a simple access breach. In total, we identify 7355 unique endpoints (56 %) that make use of the default secret.

**Cluster API.** The modular architecture of 5G core networks enables their deployment in virtual cluster environments including Kubernetes [28]. While this simplifies the deployment, the cluster architecture introduces additional security risks than can affect the core network. Open ports in the Kubernetes deployment allow an adversary to access the underlying containerization.

We test the identified endpoints for open Kubernetes and Kubelet APIs as an indicator for potential access to the underlying structure of the deployment. Overall, we find 387 instances (18 %) that expose an open Kubernetes *and* Kubelet API, and 1.5 % that has an open API for either one of them.

## 4.2. Open GTP Ports

In the analysis of open GTP ports we focus on the daily status of responsive and non-responsive endpoints. We observe that the majority of endpoints is responsive and would enable further steps as part of an attack procedure (Figure 2). This observation is stable for the covered measurement period with a constantly higher number of responsive ports.

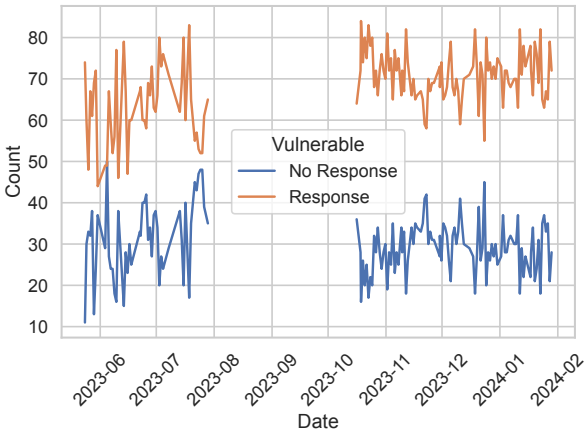


Figure 2. Daily status of the number of responsive GTP ports. Receiving a response indicates a vulnerable endpoint.

## 5. Discussion

Our findings reveal a significant number of networks that use insecure setups for their interfaces. In the following, we discuss the introduction of more security-driven default setups and address limitations of our study.

**Security-Driven Default.** Many of the threats revealed in our empirical evaluation result from the fact that the default settings for a network cannot be considered secure. To improve the overall security standard, we suggest a set of changes to the *default* configuration of the network.

A security-driven default setup must involve the use of management portals with a mandatory *custom* username and password combination. With the portals being visible and accessible on the Internet, the use of a default administrator account is highly security critical even for network deployments that are not used in production. The same applies to the use of default secrets for the protection of JWT tokens that assign administrator rights.

The standard GTP protocol does not specify any security measures that would provide additional protection beyond the default. It is, in general, recommended to use complementary security measures such as IPsec or Wireguard to restrict the access for external actors. However, such additional features go beyond simple configuration options and require additional effort for their setup. A clear documentation of recommended security measures would contribute to a higher security standard.

**Limitations.** Our measurement study does not provide any ground truth information but only focuses on technical findings. Consequently, we don't have any certainty regarding the use cases behind the network deployments, the motivation behind configuration decisions like the use of default login credentials, or contextual information regarding virtual deployments in cluster environments. Future work must address such context-related information and extend the measurement results by studies regarding the motivation behind decisions.

## 6. Conclusion

Open-source core networks provide an easy entry to the deployment of 5G campus networks. In this work, we conducted a measurement study about the current state of deployed networks focusing on the two prominent open-source implementation Open5GS and free5GC. We observed a numerous visible endpoints, of which a significant number makes use of default login credentials or assign administrator rights using the default encryption for JWT tokens. To the best of our knowledge, our measurement study is the first to assess the current state of 5G open-source networks being used in the wild. We deliver the starting point for follow-up work that should address the poor security standards of default deployments.

## References


[1] H. C. Rudolph, A. Kunz, L. L. Iacono, and H. V. Nguyen, "Security challenges of the 3gpp 5g service based architecture," *IEEE Communications Standards Magazine*, vol. 3, no. 1, pp. 60–65, 2019.

[2] Open5GS. (2024) Open-source core network implementation open5gs. [Online]. Available: https://open5gs.org/

[3] free5GC. (2024) Open-source core network implementation free5gc. [Online]. Available: https://free5gc.org/

[4] A. Alalewi, I. Dayoub, and S. Cherkaoui, "on 5g-v2x use cases and enabling technologies: A comprehensive survey," *Ieee Access*, vol. 9, pp. 107 710–107 737, 2021.

[5] T. Hoeschele, C. Dietzel, D. Kopp, F. H. Fitzek, and M. Reisslein, "importance of internet exchange point (ixp) infrastructure for 5g: Estimating the impact of 5g use cases," *Telecommunications Policy*, vol. 45, no. 3, p. 102091, 2021.

[6] "Cve-2020-8551: Denial of service vulnerability in kubelet api," https://nvd.nist.gov/vuln/detail/CVE-2020-8551, accessed: 2025-01-13.

[7] T. M. Research, "The fault in our kubelets: Analyzing the security of publicly exposed kubernetes clusters," *Trend Micro Research Blog*, 2022, accessed: 2025-01-13.

[8] "Jwt weak secret – vulnapi documentation," https://vulnapi.cerberauth.com/docs/vulnerabilities/broken-authentication/jwt-weak-secret, accessed: 2025-01-13.

[9] G. K. Gegenhuber, W. Mayer, E. Weippl, and A. Dabrowski, "MobileAtlas: Geographically decoupled measurements in cellular networks for security and privacy research," in *32nd USENIX Security Symposium*, ser. USENIX Security 23, Anaheim, CA, Aug. 2023.

[10] A. Lutu, D. Perino, M. Bagnulo, and F. E. Bustamante, "Insights from operating an ip exchange provider," in *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, 2021, pp. 718–730.

[11] A. Özgü *et al.*, "monroe: Measuring mobile broadband networks in europe," in *Proceedings of the IRTF & ISOC Workshop on Research and Applications of Internet Measurements (RAIM)*, 2015.

[12] F. Li, A. A. Niaki, D. Choffnes, P. Gill, and A. Mislove, "A large-scale analysis of deployed traffic differentiation practices," in *Proceedings of the ACM Special Interest Group on Data Communication*, ser. SIGCOMM '19. New York, NY, USA: Association for Computing Machinery, 2019.

[13] D. Dauphinais, M. Zylka, H. Spahic, F. Shaik, J. Yang, I. Cruz, J. Gibson, and Y. Wang, "automated vulnerability testing and detection digital twin framework for 5g systems," in *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*. IEEE, 2023, pp. 308–310.

[14] S. Luo, J. Wu, J. Li, L. Guo, and B. Pei, "toward vulnerability assessment for 5g mobile communication networks," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*. IEEE, 2015, pp. 72–76.

[15] C.-T. Kuo, H.-Y. Chen, and T.-N. Lin, "rain: Risk assessment framework based on an interdependent-input propagation network for a 5g network," *IEEE Access*, 2023.

[16] H. A. Kholidy, "multi-layer attack graph analysis in the 5g edge network using a dynamic hexagonal fuzzy method," *Sensors*, vol. 22, no. 1, p. 9, 2021.

[17] R.-G. Lazar, A.-V. Militaru, C.-F. Caruntu, C. Pascal, and C. Patachia-Sultanoiu, "real-time data measurement methodology to evaluate the 5g network performance indicators," *IEEE Access*, 2023.

[18] S. R. Group *et al.*, "a global perspective of 5g network performance.(2019)," *Retrieved June*, 2020.

[19] D. Xu, A. Zhou, X. Zhang, G. Wang, X. Liu, C. An, Y. Shi, L. Liu, and H. Ma, "Understanding operational 5g: A first measurement study on its coverage, performance and energy consumption," in *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, ser. SIGCOMM '20. New York, NY, USA: Association for Computing Machinery, 2020.

[20] J. Rischke, P. Sossalla, S. Itting, F. H. Fitzek, and M. Reisslein, "5g campus networks: A first measurement study," *IEEE Access*, vol. 9, pp. 121 786–121 803, 2021.

[21] I. Shayea, M. H. Azmi, M. Ergen, A. A. El-Saleh, C. T. Han, A. Arsad, T. A. Rahman, A. Alhammadi, Y. I. Daradkeh, and D. Nandi, "performance analysis of mobile broadband networks with 5g trends and beyond: Urban areas scope in malaysia," *IEEE Access*, vol. 9, pp. 90 767–90 794, 2021.

[22] J. Isabona, C. C. Ugochukwu, A. L. Imoize, and N. Faruk, "an empirical comparative analysis of 4g lte network and 5g new radio," in *2022 5th Information Technology for Education and Development (ITED)*. IEEE, 2022, pp. 1–5.

[23] M. Barbosa, M. Silva, E. Cavalcanti, and K. Dias, "Open-source 5g core platforms: A low-cost solution and comparative study of open5gs and free5gc," *arXiv preprint arXiv:2412.21162*, 2024, accessed: 2025-01-13. [Online]. Available: https://arxiv.org/abs/2412.21162

[24] T. Mukute, L. Mamushiane, A. A. Lysko, E.-R. Modroiu, T. Magedanz, and J. Mwangama, "Control plane performance benchmarking and feature analysis of popular open-source 5g core networks: Openairinterface, open5gs, and free5gc," *IEEE Access*, 2024.

[25] T. Tervoort, "Three new attacks against json web tokens," Black Hat USA 2023, 2023, accessed: 2025-01-13.

[26] Shodan. (2024) Shodan search engine. [Online]. Available: https://www.shodan.io/

[27] Censys. (2024) Censys search engine. [Online]. Available: https://search.censys.io/

[28] H. Bäckström and R. Bohra. (2022) Why kubernetes over bare metal infrastructure is optimal for cloud native applications. [Online]. Available: https://www.ericsson.com/en/blog/2022/5/kubernetes-over-bare-metal-cloud-infrastructure-why-its-important-and-what-you-need-to-know


## Appendix

The observed endpoints in the data set are defined through their geographical distribution and their overall uptime within the measurement period. We document both characteristics in the following.

**Geographical Characteristics.** We derive the approximate location of endpoints from GeoIP information and observe overall 34 individual countries. The top five countries represented in the measurements are the US, India, Taiwan, China, and Germany.

**Uptime.** We use the occurrence of management portals in our results as an indicator for the uptime of networks. To this end, we analyze the uptime by deriving the number of days each IP address is visible during the daily measurements. Although there is no ground truth regarding the real uptime or the purpose of the endpoint, we can still use this information to get a first idea of the observed landscape of deployed networks. In our dataset, we see a median uptime of 16 days with a minimum of one day and a maximum of 250 days. Please note that IP addresses are not necessarily permanent and only serve as an indicator for the uptime.