5G SECURITY TEST BED™

Securing 5G:

Network Slicing Phase 2 Test Report

5G Security Test Bed's Network Slicing Tests Strengthen 5G Security

Spring 2024

Table of Contents

Introduction 3
Scope of Report 4
Background 4
Network Slicing 4
Network Slice Identifiers 5
Definition of Test Cases 5
Test Results 7
Summary of Process and Findings 7
Test Case 1: Malicious Access to a Different Slice by Modifying Slice Differentiator 7
Test Case 2: Static Subscriber S-NSSAI Override of UE-Requested NSSAI by Dynamic Core Signaling Assignment 15
Conclusions and Next Steps 20
Summary of Test Results 20
5G Security Test Bed Strengthened 3GPP Standards 20
Next Steps 21
About the 5G Security Test Bed 22
Appendix: Acronyms 24
References 25

Introduction

The 5G Security Test Bed Is Designed to Rigorously Test and Advance 5G Security

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. With 5G in particular, secure connectivity is the foundation that supports and enhances the many benefits these networks provide. The wireless industry devotes significant resources to 5G security and has expanded its efforts through the 5G Security Test Bed.

Formally launched in 2022, the 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, created with a sole focus on testing and validating 5G security recommendations and use cases from government groups, wireless operators, and others. It is the only initiative that uses commercial-grade network equipment and facilities to demonstrate and validate how 5G security standards recommendations will work in practical, real-world conditions.

One of the 5G Security Test Bed's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the Test Bed's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G Security Test Bed's previous testing activities have worked to validate the recommendations of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) advisory group, for both non-standalone (NSA) and standalone (SA) network configurations. In addition, the Test Bed draws on recommendations from its own Technical Advisory Committee to address emerging industry priorities.

This report addresses network slicing security on 5G networks, adding to three previous test cases conducted in the Phase 1 network slicing report released in 2023.[i] The 5G Security Test Bed will continue evaluating additional recommendations and use cases from CSRIC and other entities in future tests. It is not set up to be a platform for identifying vulnerabilities or conducting penetration testing of networks or equipment.

Scope of Report

This 5G Security Test Bed report's scope is to demonstrate potential exploits that result from network slicing vulnerabilities outlined in the AdaptiveMobile Security (AMS) white paper *A Slice in Time: Slicing Security in 5G Core Networks*, submitted to GSMA as a Common Vulnerability Disclosure (CVD).[ii] While the vulnerability was theoretical in the AMS paper, the Test Bed replicated the hypothetical exploit outlined in the report on its own live network infrastructure. The Test Bed also developed and tested an additional potential exploit based on the vulnerability.

These two test cases—the first to validate and assess this theoretical vulnerability using real-world testing—along with the AMS report, led to the 3rd Generation Partnership Project (3GPP) updating the 5G network technical specifications found in TS 33.501, Version 18,[iii] resolving the vulnerability.

Background

Network Slicing

Network slicing is a technology that enables mobile network operators to provide fine-grained, customizable network offerings to meet the diverse needs of a variety of customers and applications, such as in public safety, transportation, security, and many other contexts.

Often, network slices are discussed in the context of leading commercial applications, such as the four wireless network service types defined by 3GPP: eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communication), mMTC (Massive Machine-Type Communication), and Vehicle to X (V2X). In addition, network slices for specific uses, such as vehicle-to-infrastructure, or a specific company's industrial control system, are also considered for application of the network slicing concept.

Network slices can be viewed as logical networks sharing a common physical infrastructure. The security for network slicing will be critical to certain segments of commercial customers. Regarding network slice security, because network slices leverage network function (NF) virtualization and a service-oriented architecture, the main focus for slice security has been to ensure isolation among different slices. Specifically, there are two aspects of isolation: resource provision/isolation and security isolation. Security isolation not only requires slice-specific access control and security measures, but also ensures that potential problems in one slice will not spill over to other slices.

Network Slice Identifiers

In the 5G network core, each slice is given a unique identity called the Single-Network Slice Selection Assistance Information (S-NSSAI). The S-NSSAI is used to identify, differentiate, authorize, and route each slice and the data traveling on it. The S-NSSAI identifies each slice in two parts: a mandatory Slice Service Type (SST), which is a predefined value for one of the wireless network service types defined by 3GPP listed above, and an optional Slice Differentiator (SD), which is used to differentiate between slices of the same type.

In some cases, user equipment (UE) may be authorized to access more than one slice, and the network further differentiates these with a group or list of up to eight slices identified by Network Slice Selection Assistance Information (NSSAI). NSSAIs can fall into several categories, including Allowed, Rejected, Configured, or Requested NSSAIs.

AdaptiveMobile's 2021 CVD Report, *A Slice in Time: Slicing Security in 5G Core Networks*, noted that there was no requirement for mobile network operators (MNOs) that each slice has a unique identifier, or that Slice Differentiators be random, adding that, "With all the new network functions and services in 5G, roaming and legacy interaction will become quite complex."

3GPP's technical standards on network slicing note that "the subscription information shall include at least one default S-NSSAI," requiring network operators to include a default described S-NSSAI in the subscriber slice profile for the UE. However, with no guidance for interoperability between vendors in 3GPP's technical standards at the time of AdaptiveMobile's report release, *A Slice in Time* highlighted security challenges through configuration mistakes and missing layer matching. The report listed some hypothetical examples, showing how slices could potentially be manipulated to do more than they should be able to do, including by brute forcing or guessing slice identifiers to access unauthorized information or resources within the network.

Definition of Test Cases

Based on guidance from its Technical Advisory Committee and the AdaptiveMobile report, the 5G Security Test Bed wrote and executed two tests to demonstrate whether the theoretical vulnerability could be exploited in a real-world environment.

In the first potential exploit outlined in the report, "Malicious Access to a Different Slice by Modifying Slice Differentiator," a rogue network function or a rogue slice (Slice 2 in this example) from a compromised partner could theoretically establish a TLS connection that appears valid because it is using the correct slice identity. This rogue slice would then be allowed to access the network function shared with the valid Slice 1 and granted a valid identification token. With this access token, the network's transport/IP layer security would determine the rogue slice is a valid connection, granting it access to personal data or resources within the network.

The report discusses the cause of the vulnerability:

> *The underlying problem is that no layer matching is mandated by the specifications. As there is no matching between layers, the NRF would only see, on the lower transport/IP layer, an "authenticated partner" and, on the upper signalling layer, a valid slice identity and service request. There is no cross-check that the slice identity in the request matches the slice identity used for the TLS tunnel. As a result, the NRF would issue an authorization ticket to the rogue Slice 2 to use services on Slice 1.*

The 5G Security Test Bed performed the first real-world tests to confirm whether this hypothetical vulnerability could be exploited, listed in this report as Test Case 1. In addition, the Test Bed developed a second test case based on the vulnerability, "Static Subscriber S-NSSAI Override of UE-Requested NSSAI by Dynamic Core Signaling Assignment," or referred to more simply as "5G Network Override to Reroute a Mis-Provisioned Network User Slice."

In Test Case 2, the Test Bed assumed that a user device had been incorrectly provisioned to a network slice that was inconsistent with how it was recorded by the network operator. In this example, the UE should be provisioned for Slice 2, but it incorrectly presents Slice 1 as the Requested NSSAI to the network. Test Case 2 was conducted to determine whether the network would override the incorrect request and direct the UE to the correct slice.

In summary, the 5G Security Test Bed conducted the following tests:

1. Malicious Access to Different Slice by Modifying Slice Differentiator
    a. 5G STB Test Case 1: Confirm the vulnerability by executing a successful modified request first from the compromised network function (NF) to the network repository function (NRF), and then to the shared NF.

2. Static Subscriber S-NSSAI Override of UE-Requested NSSAI by Dynamic Core Signaling Assignment
    a. 5G STB Test Case 2: Test and validate the cellular network's ability to override a mis-provisioned, mis-configured, or manipulated user device (UE) that has the network slice provisioned for Slice 1 where it should be Slice 2.

The vulnerability outlined by AdaptiveMobile is a niche edge case that requires a very specific set of circumstances to occur and would be difficult to execute in the real world. However, by confirming with real-world tests and disclosing the findings to 3GPP, the 5G Security Test Bed helped drive the development of updated standards to address the potential issue and override the vulnerability.

Test Results

Summary of Process and Findings

The configuration used for these tests is comprised of radio access network (RAN) equipment hosted at the University of Maryland (UMD) and a dual-mode core (DMC), which provides both 4G LTE and 5G functionality hosted at the MITRE Corporation. The connection between the RAN at UMD and the DMC at MITRE goes over the internet. The DMC is an Ericsson 5G Core, PCC version 1.19.

The core is configured to support two network slices. Mutual TLS (mTLS) is implemented among network functions.

Tests were run with band N41 for the new radio (NR), using a Sierra Wireless EM9190 card connected to a laptop by USB as a cellular modem, as well as a Qualcomm Mobile Test Platform (MTP) device. For the purposes here, this report refers to the combination of that laptop and the cellular modem as the UE. The UE used for Slice 1 was the Qualcomm MTP. It was set inside a Faraday Cage and connected remotely through a laptop.

Test Case 1: Malicious Access to a Different Slice by Modifying Slice Differentiator

Test Case ID: TC-NetSlic-01
Description:
Test Case 1 is designed to confirm the existence of the vulnerability reported by AdaptiveMobile in Section 3.1.3.1 of its report, *A Slice in Time: Slicing Security in 5G Core Networks* (submitted to GSMA as CVD-2021-0047). To confirm the vulnerability, the test's objectives are to use a compromised network function belonging to Slice 2 to send a modified request to the NRF, gain access to a valid authentication token, and then use that token to access a network function shared between both Slice 1 and 2, gaining access to personal user data or resources.

This test uses the SMF network function in Slice 2 as the compromised NF, and it uses the AMF as the network function that is shared between both slices. It then uses the Namf_Communication_N1N2MessageTransfer service request to attempt to release an existing connection that the UE in Slice 1 is connected to in order to see if the AMF will respond to this maliciously crafted request.

The test uses Ericsson's internally developed HTTP/2 and REST API call interception and modification tool called HALO. The tool operates as a man-in-the-middle that can inspect the HTTP/2 requests and responses. Using HALO, requests and responses can be modified in the HTTP/2 Body, within the JSON or any payload type, the HTTP/2 Headers, and the URI query parameters. For the test, HALO sits outside the 5G network core, and traffic is directed to HALO

by configuring the IP addresses of the AMF and the NRF to be interfaces on HALO. HALO masquerades as the SMF on Slice 2, generating and receiving messages as appropriate. HALO is capable of having a PKI certificate for the core installed, and it can decode TLS traffic. It also has the Wireshark capability to capture traffic in PCAP format. With mTLS implemented, everything is encrypted between NFs. As a result, Wireshark captures from outside HALO cannot read the contents of messages. In order to display message content, we need to read them (and modify and/or generate them) inside HALO, where they have been decrypted.

Prior to executing the test below, HALO snoops the connection PDU setup for the UE in Slice 1 in order to gather the needed parameters to craft the malicious REST API call to release the connection from Slice 2.

A number of features are configured for the test case in the Service-Based Architecture (SBA) of the 5G core in addition to mutual TLS using PKI certificates. The NRF acts as the OAuth 2.0 Authorization server and generates the Access Token Response, which is a JWS-signed JSON object containing the access token, a token type, expiration, and scope, which is per REST API service. Tokens are authorized per REST API service for the NF where one side acts as the NF service consumer and the other NF acts as the NF service producer. The tokens generated by the NRF authorize the Namf_Communication_N1N2MessageTransfer service to be used between the SMF as the NF service consumer, and the AMF as the NF service producer, as an example in this test case.

This test case recognizes that the above scenario is difficult in the real world to execute, but the purpose is to test the layer matching problem highlighted by Adaptive Mobile. The actual testing is constrained by the actual supported REST APIs for the SMF to the AMF, which are limited in the current software to the Namf_Communication_N1N2MessageTransfer service, the N1N2Transfer Failure Notification service, and the EBIAssignment service. These allow for only PDU session establishment, modification, and release operations. Additional software releases add more REST API services.

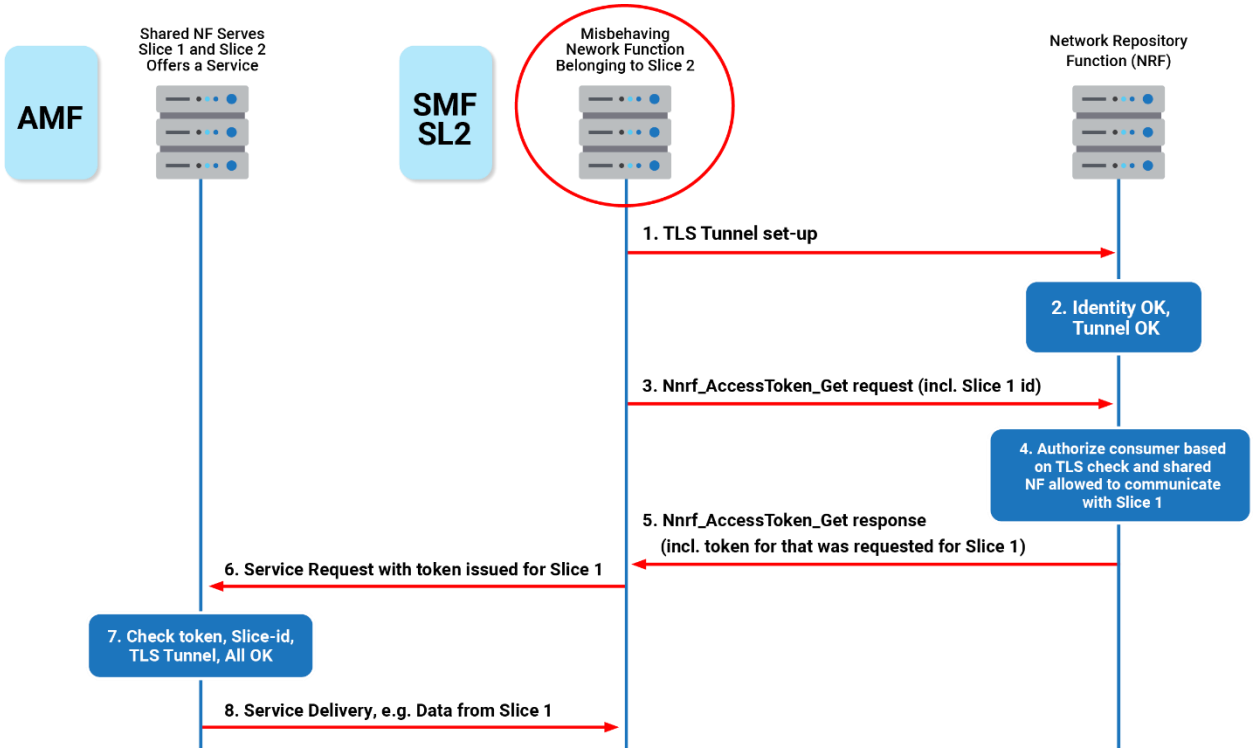

Figure 1: Message Flow of Hypothesized Vulnerability

Because packet captures occur inside the HALO tool, the IP addresses associated with the messages are in some cases the internal HALO IP addresses facing the NFs. The relevant IP addresses are listed in Table.

Table: Network Function IP Addresses

AMF	NRF	SMF
192.168.56.143	192.168.56.143	192.168.56.129
172.17.20.108 (HALO)	172.17.95.197 (HALO)	192.168.56.131
	172.17.96.50 (HALO)	

Prior to conducting the test, the UE is connected to Slice 1 and establishes a data connection to the Slice 1 server. Figure 2 shows the UE registration in which it provides its Subscription Concealed Identifier (SUCI) (310014791791003), and Figure 3 is the UE establishing its PDU session (PDU Session ID 1) on Slice 1 (SST=1, SD=1). HALO captures the PDU session establishment in order to use the needed parameters to craft the malicious REST API call to release the PDU session later in the test.

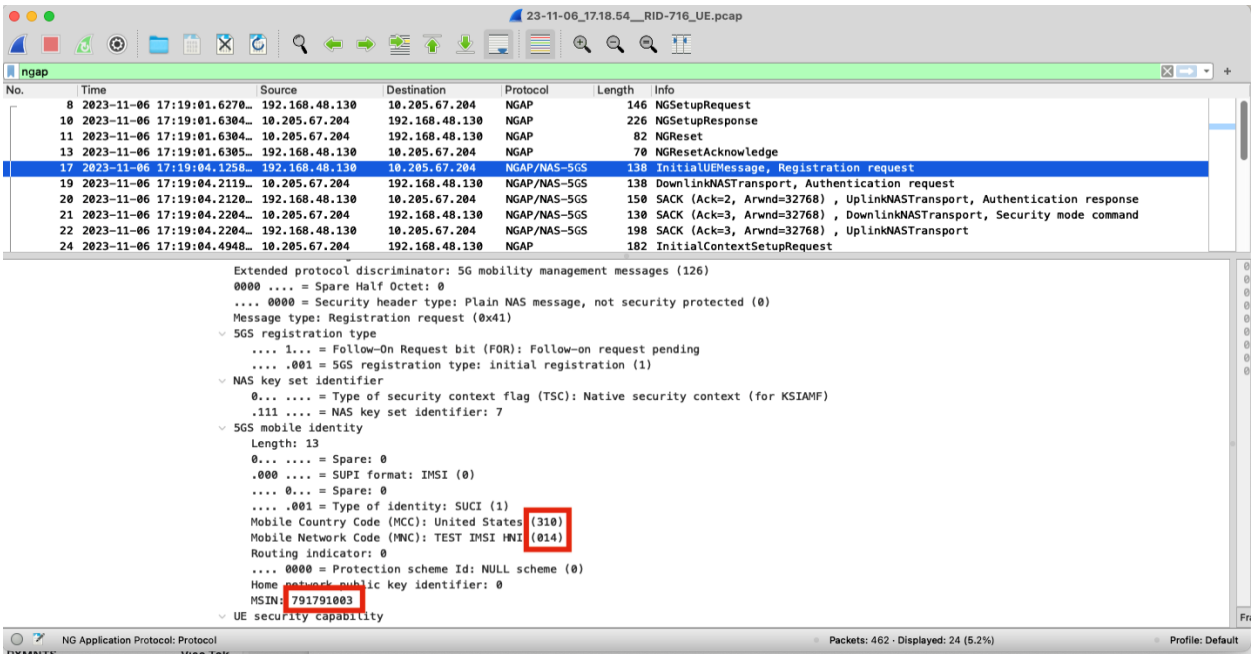

Figure 2: UE Registration Showing SUCI

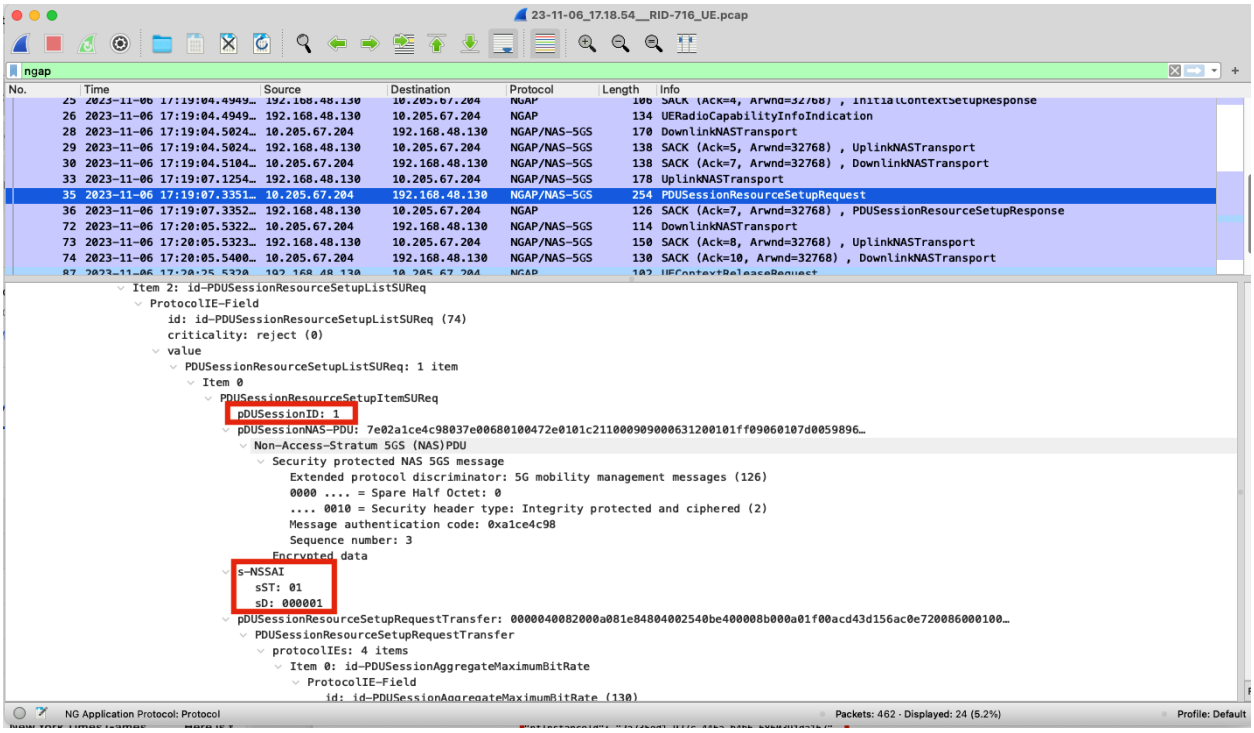

Figure 3: UE PDU Session Setup Request Showing pDUSessionID and s-NSSAI

HALO performs the function of the rogue NF, the SMF, on Slice 2. Figure 4 shows the NF instance details of this NF, including NF type (SMF) and NSSAI (SST=1, SD=2).

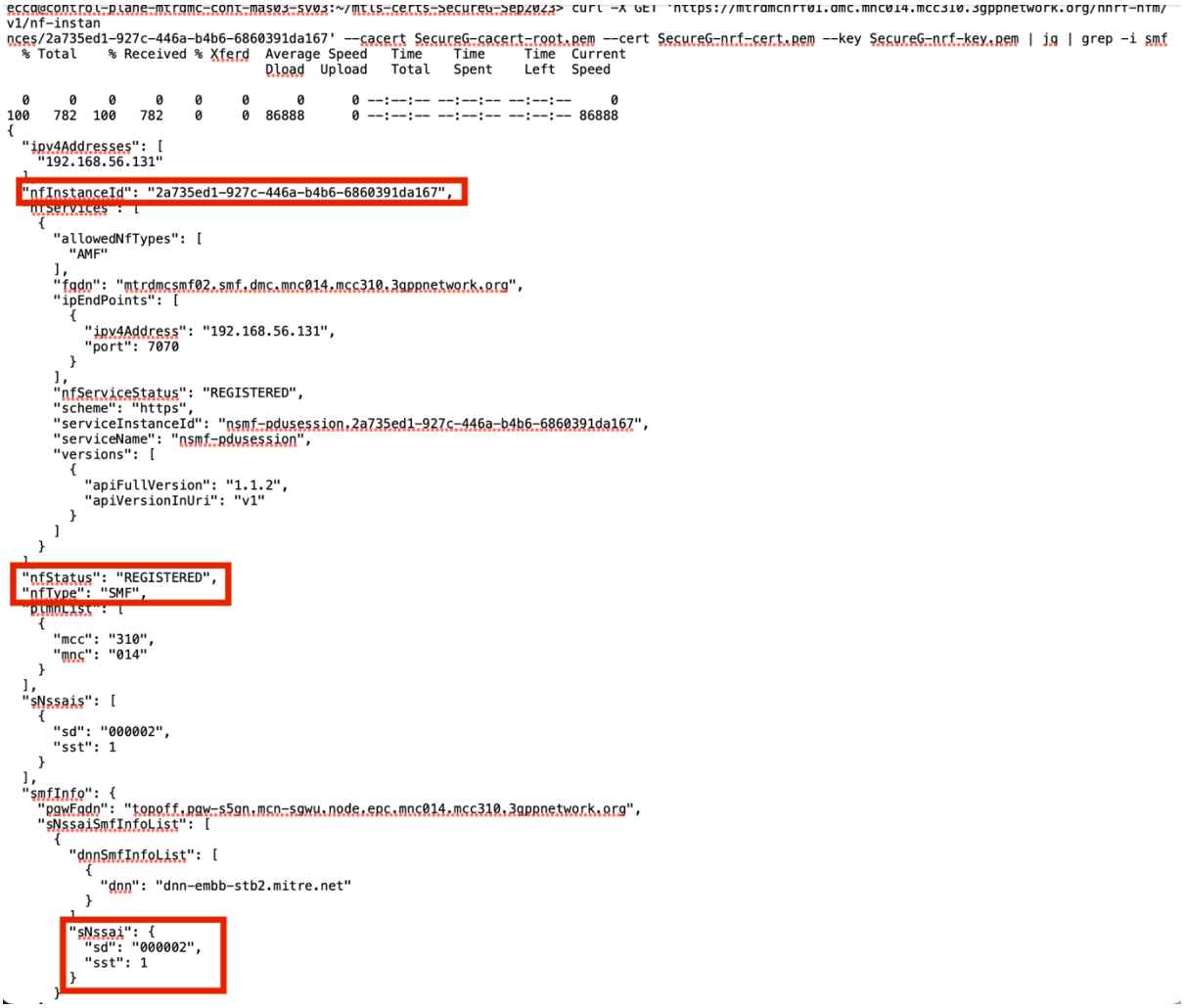

Figure 4: Compromised NF (SMF) Parameters (nfType, sNssai, etc.)

HALO, masquerading as the compromised SMF on Slice 2, establishes a TLS connection to the NRF to request access to the AMF shared by both Slice 1 and Slice 2. HALO then sends a request to the NRF to provide the rogue SMF a token to access Slice 1 on the shared NF server. In this test case execution, the slice for which the request corresponds is not included in the request, as targetSnssaiList is optional in the AccessTokenReq. Line 56 of Figure 5 shows the rogue SMF (the IP address appears as 172.17.96.50, which corresponds to the HALO interface facing the NRF) requesting the AMF access token from the NRF (192.168.56.143), where the nfInstanceId matched that in Figure 4. Note the details in the request do not include the targetSNSSAIList. Line 60 of Figure 6 shows the NRF (192.168.56.143) returning the AMF access token without any specific S-NSSAI listed. The scope allows access to the Namf_Communication_N1N2MessageTransfer service.

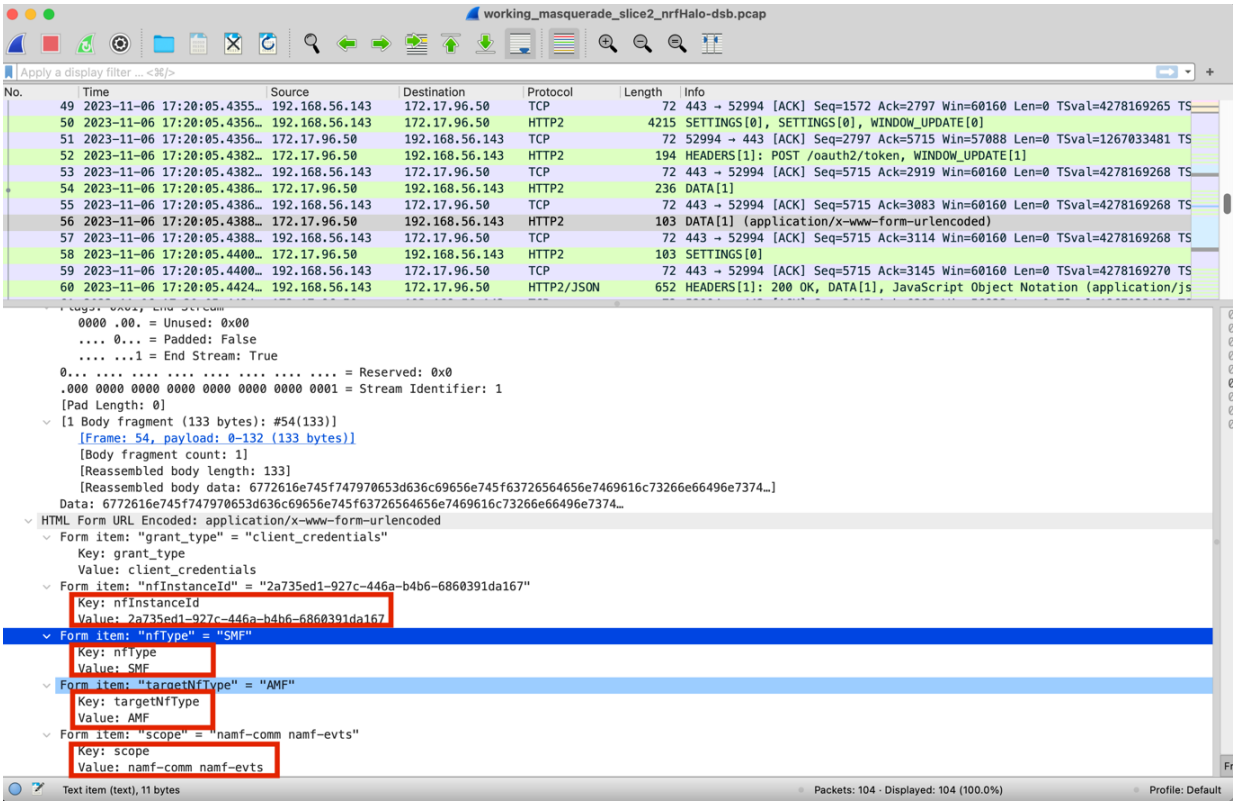

Figure 5: Wireshark Capture of Rogue SMF Request to NRF for AMF Token

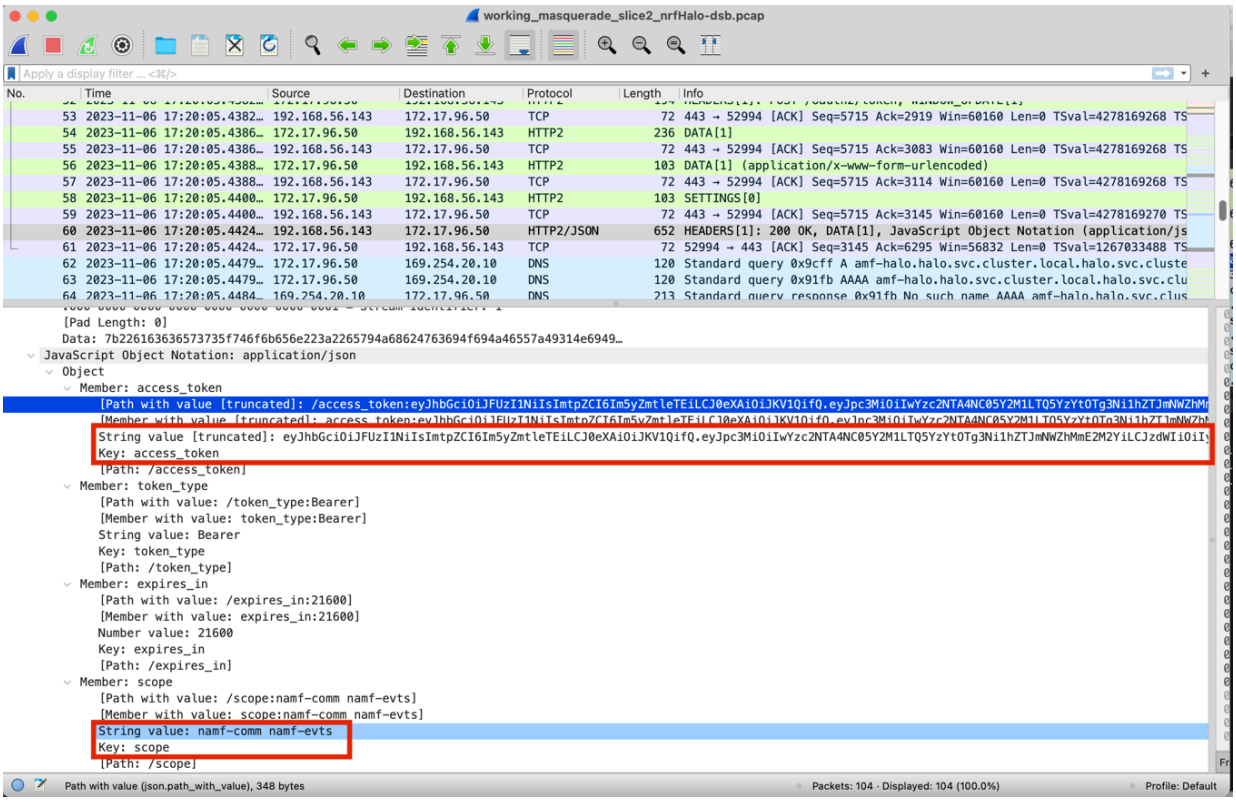

Figure 6: NRF Response to Rogue SMF providing AMF Token

Next, HALO, again masquerading as the rogue SMF on Slice 2, presents to the shared AMF network function the AMF access token that does not specify a particular slice. Line 24 of Figure 7 shows an HTTP/2 POST specific to the UE on Slice 1 (SUCI/IMSI 310014791791003), providing to the AMF (172.17.20.108) the AMF access token received from the NRF as shown in Figure 6. Subsequently, HALO uses the Namf_Communication_N1N2MessageTransfer service for the rogue SMF to initiate a Request to Release the existing PDU connection using the needed parameters acquired by snooping the PDU session setup prior. Line 28 of Figure 8 shows the message to the AMF (172.17.20.108) requesting the release of PDU Session ID 1, the PDU session associated with the UE as originally established in Figure 3.

Finally, Figure 9 shows the UE packet capture in which the UE receives the PDU session release command. The PDU session is then released and torn down.

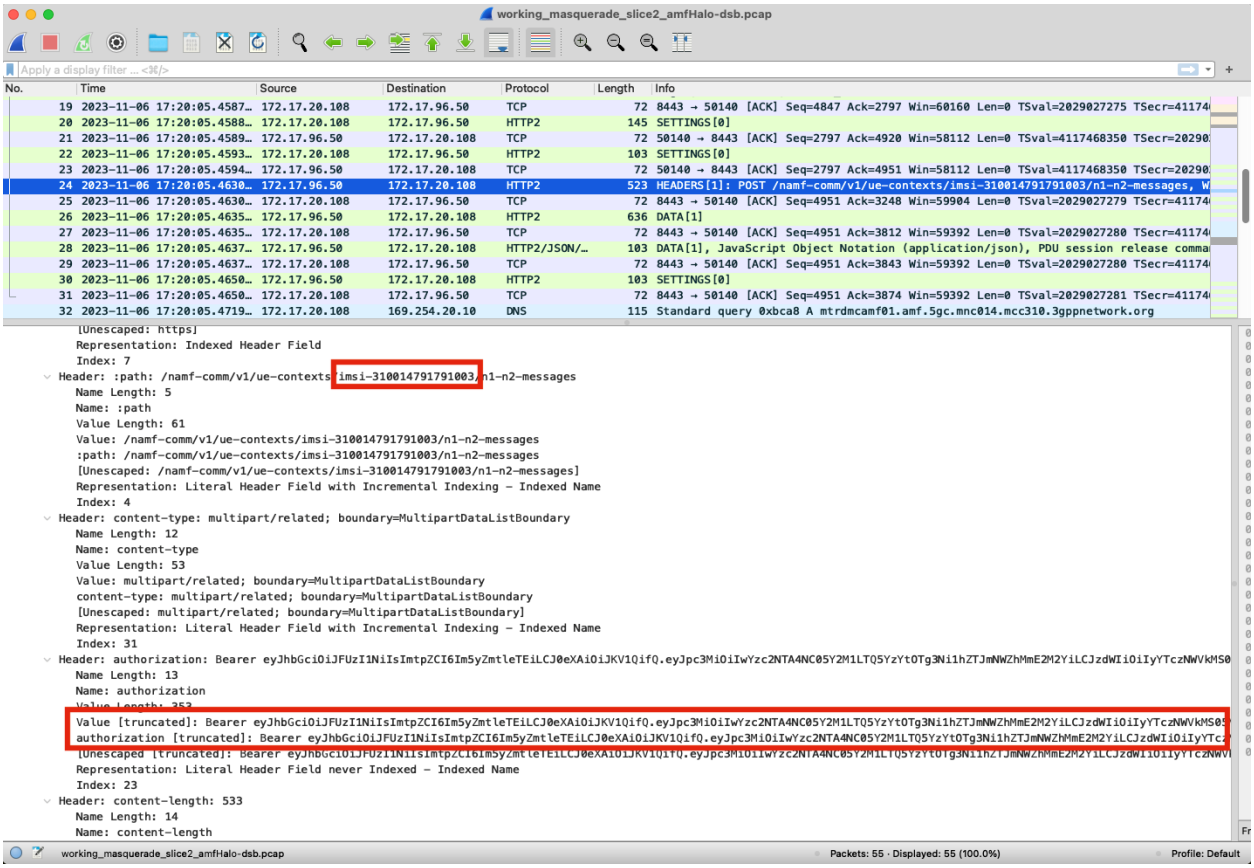

Figure 7: Rogue SMF Presentation of AMF Access Token to AMF

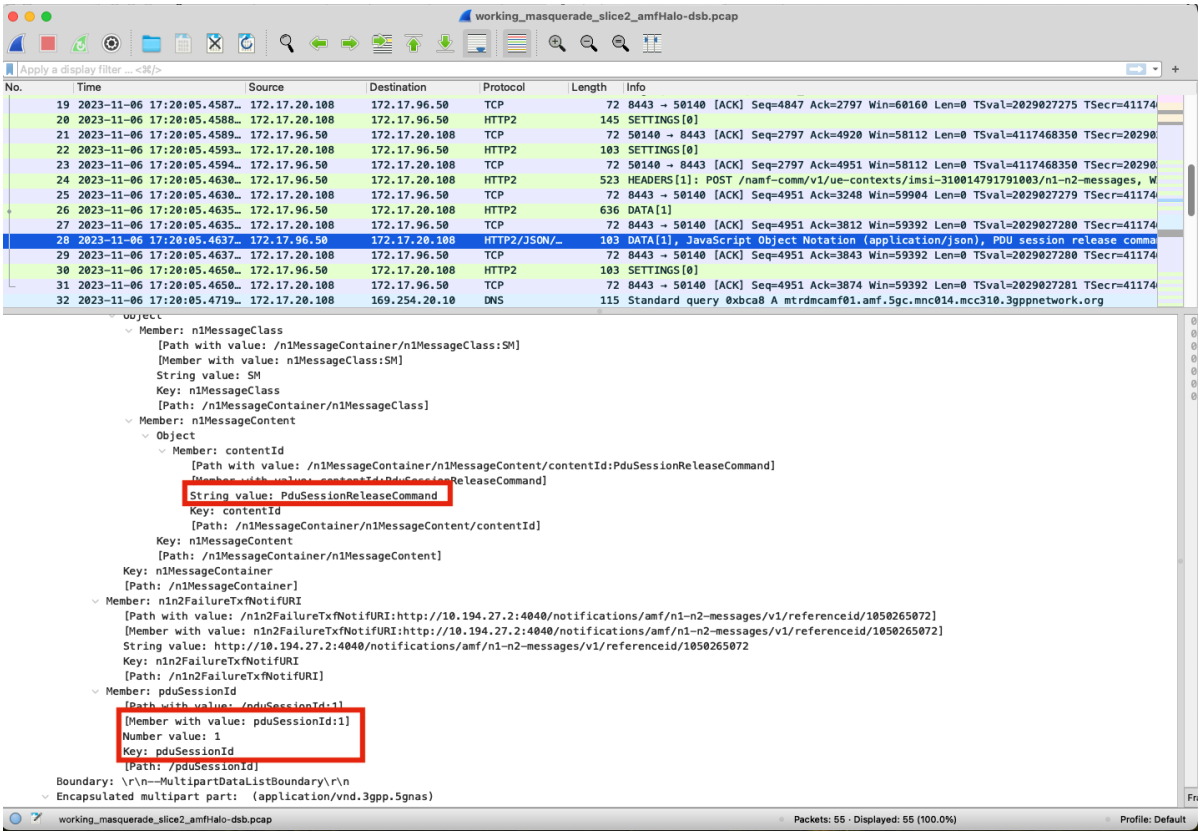

Figure 8: PDU Session Release Request from Rogue SMF

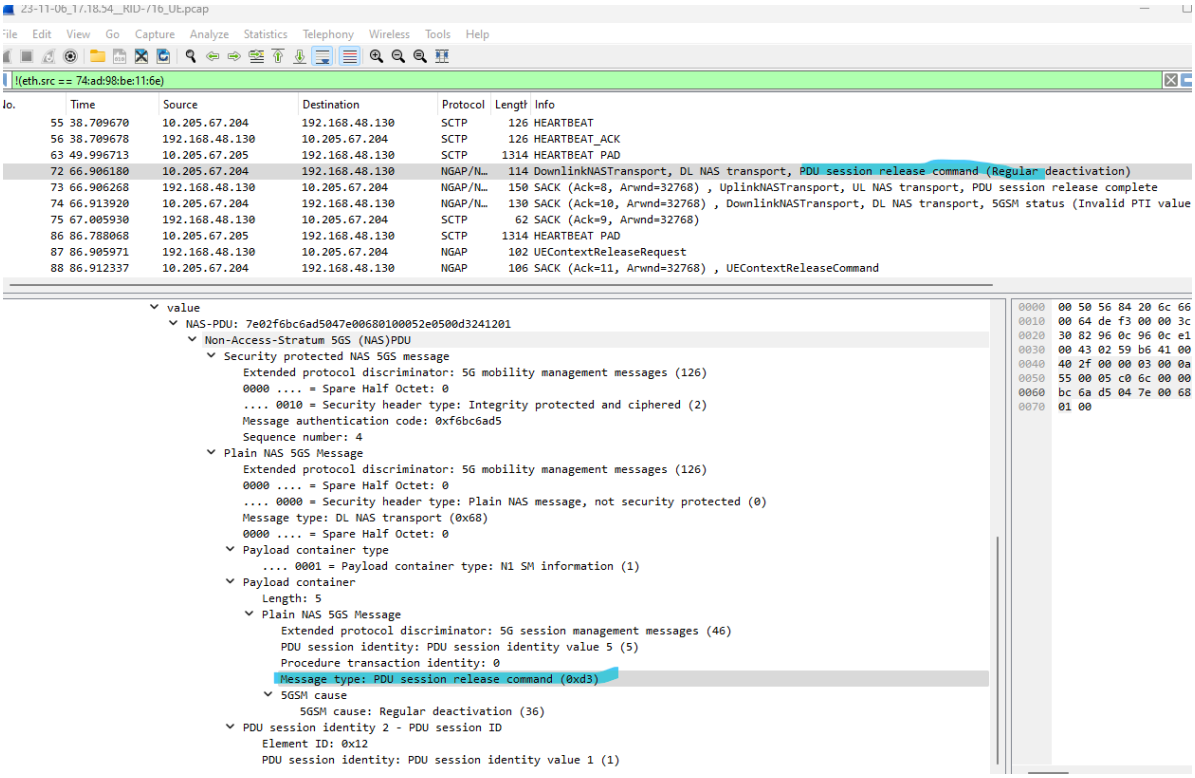

Figure 9: UE Packet Capture Showing PDU Session Release Command

Expected Results:

1. The compromised NF is allowed to access the AMF shared network function, and a valid token for the shared AMF NF is generated by the NRF. The token contains the AuthenticationTokenClaims, which define the scope of the token for the Namf_Communication_N1N2MessageTransfer service. The token is sent to the Compromised SMF Test NF by the NRF.
2. The Shared AMF NF responds to the maliciously crafted REST API call and releases the PDU session, thus indicating that the vulnerability exists.

Results:

Success Criteria	Status
A valid token for the shared AMF NF is generated by the NRF and provided to the rogue NF.	The NRF, in response to a request from the rogue SMF on Slice 2, without any slice specified in request, provides the AMF an access token without slice restriction.
The token contains the AuthenticationTokenClaims.	The NRF-generated token includes namf-comm and namf-evts in scope.
Shared AMF NF responds to the maliciously crafted REST API call and releases the PDU session, thus indicating that the vulnerability exists.	After the rogue SMF sends a PDU session release request to the AMF for the UE on Slice 1, the UE receives a PDU session release command and tears down the PDU session.
Overall Test	Confirmed

Test Case 2: Static Subscriber S-NSSAI Override of UE-Requested NSSAI by Dynamic Core Signaling Assignment

Test Case ID: TC-NetSlic-02

Description:

The purpose of this test case, which can also be called “5G Network Override to Reroute a Mis-Provisioned User Slice,” is to validate the ability of the cellular network to override a mis-provisioned, mis-configured, or manipulated user device (UE) that has the network slice provisioned inconsistently with how it is recorded by the network operator.

In this test, the UE presents Slice 1 as the Requested NSSAI to the network. However, the UE subscription data in the UDM/UDR has the proper provisioning for Slice 2. Slice 2 is configured as the default subscribed S-NSSAI in the UDM Slice Profile, and this setting is expected to override the Requested NSSAI given by the UE to the network.

The AMF is the network function that performs this override function as it retrieves the subscribed S-NSSAI from the UDM and sends to the UE the Allowed and Configured NSSAI, which includes the subscribed S-NSSAI in order to ensure that the network wins in a mismatch. The Rejected NSSAI is not sent as this is used for the Serving PLMN in a roaming scenario. These exchanges are defined in 3GPP TS 23.501.[iv] The exchange of information is shown in Figure 10.

Note: Depending on the UE implementation, the Allowed NSSAI information that was once received during registration might be permanently stored on the device and be used to compose the Requested NSSAI in any following registration procedures including the initial registration after a UE power off-on cycle.

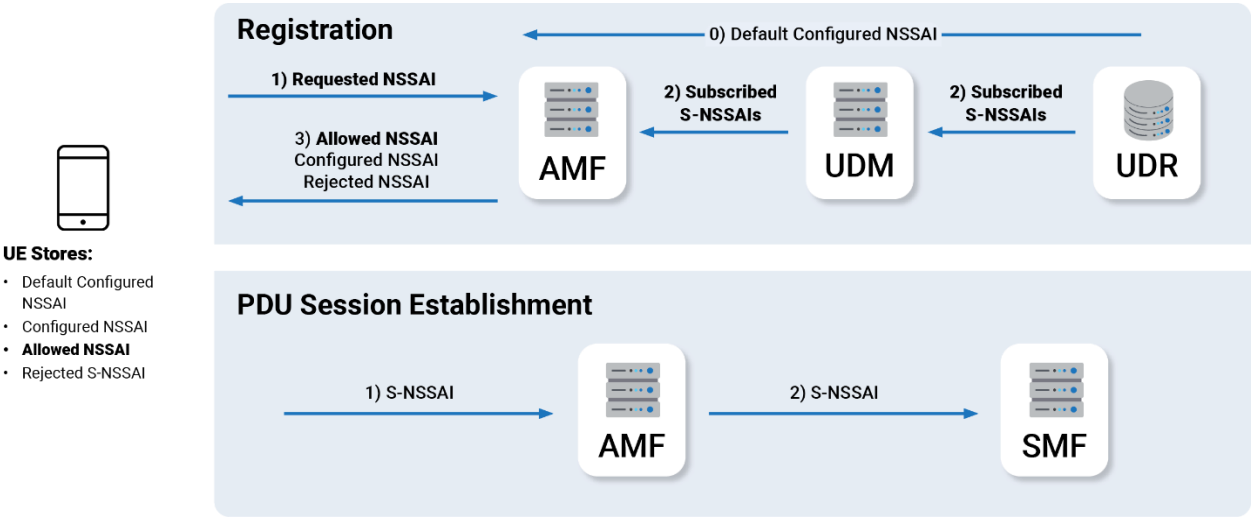

Figure 10: Slice Selection and Use

In the executed test, the UE was provisioned with a SIM card dedicated in the core network to slice configuration SST=1 and SD=2; however, the SIM card itself was configured for slice configuration SST=1 and SD=1. It had not previously attached to the 5G core with this SIM card. As shown in Figure 11, the IMSI was 310014791791022 and the IMEI was 351735110121742. From Figure 12, we confirm the default configured NSSAI as SST=01, SD=000001. Also, as expected, it does not contain any PLMN values.

```
Manufacturer: Sierra Wireless, Incorporated
Model: Sierra Wireless EM9190
Firmware:     03.09.06.00_GENERIC
Network type: GSM
Data class:   UMTS, HSDPA, HSUPA, LTE, 5G-NSA, 5GSA/TDS
IMEI:  351735110121742
Mobile number:      7917910022
IMSI:  310014791791022
SIM ICCID:    89010020000011163739
```

Figure 11: UE SIM Card Details

```
OK
AT+CGDCONT?
+CGDCONT: 1,"IP","","0.0.0.0",0,0,0,0,,,,,,,,,"",,,,0
+CGDCONT: 2,"IPV4V6","","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0,,,,,,,,,"",,,,0

OK
AT+C5GNSSAIRDP=0
+C5GNSSAIRDP: 4,"01.000001"

OK
AT+C5GNSSAIRDP=3
+C5GNSSAIRDP: 4,"01.000001"

OK
AT+C5GNSSAIRDP=2
+C5GNSSAIRDP: 4,"01.000001"
```

Figure 12: SIM NSSAI Details from AT Command

The test started with the UE in airplane mode. Upon exiting airplane mode, the UE attached to the 5G network. During the attach process, we collected attach logs data for the UE, and slice information using AT (attention) commands.

Figure 13 shows the UE-requested NSSAI details from the Registration Request message in packet 1620, indicating the requested S-NSSAI=1, SST=1, and SD=1. However, the NSSAI details from Core downlink Registration Accept message shows both the Allowed NSSAI and Configured NSSAI as S-NSSAI=1 and SST=1, but the SD has changed to SD=2 (see Figure 14, packet 1633).

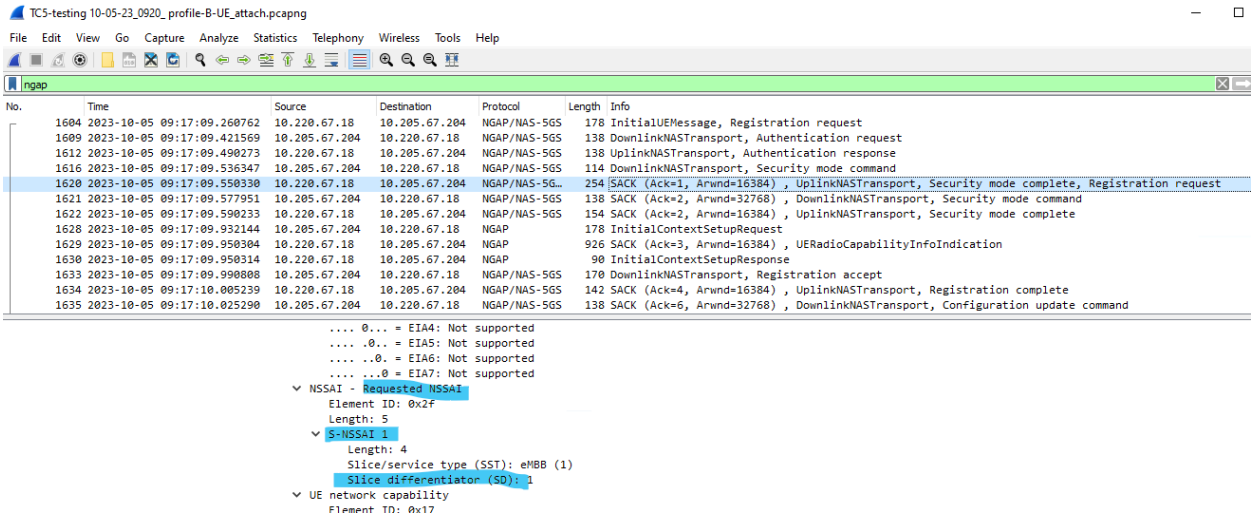

Figure 13: NSSAI Details from UE Registration Request Message

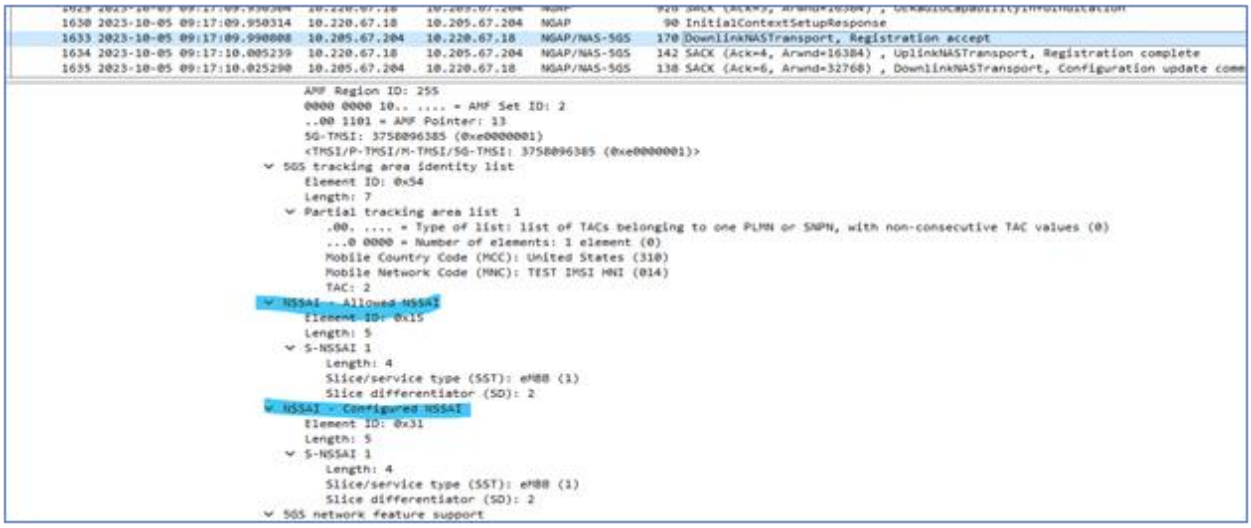

Figure 14: NSSAI Details from Core Downlink Registration Accept Message

Figure 15 shows how, after the UE attached, the SIM subsequently displayed PLMN=310014 and was configured with NSSAI as SST=01 and SD=000002, as well as Allowed NSSAI SST=01, SD=000002. Note the SD values differ from the original SIM configuration and match the configuration in the core.

```
AT+C5GNSSAIRDP=3
+C5GNSSAIRDP: 4,"01.000001"
+C5GNSSAIRDP: "310014",4,"01.000002",4,"01.000002"

OK
AT+C5GNSSAIRDP=2
+C5GNSSAIRDP: 4,"01.000001"
+C5GNSSAIRDP: "310014",4,"01.000002"

OK
AT+C5GNSSAIRDP=0
+C5GNSSAIRDP: 4,"01.000001"

OK
AT+CGDCONT?
+CGDCONT: 1,"IP","","0.0.0.0",0,0,0,0,,,,,,,,,"",,,,0
+CGDCONT: 2,"IPV4V6","","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0,,,,,,,,,"",,,,0

OK
```

Figure 15: SIM NSSAI Details from AT Command after Successful UE Attach

Expected Results:

1. When the UE registers to the 5GS, the Requested NSSAI for Slice 1 is seen in the NAS REGISTRATION REQUEST message.
2. The AMF provides the UE with the Allowed and Configured NSSAI information as well as the NSSAI inclusion mode in the NAS REGISTRATION ACCEPT message. The AMF should embed Slice 2 in this information, which it received from the UDM slice profile. This will override the Requested NSSAI Slice 1 from the UE. This will be seen using the Software Probe in the PCC for the N2 interface.
3. The UE is connected to Slice 2.

Results

Success Criteria	Status
The UE, though provisioned with a Requested NSSAI for Slice 1, is overridden by the network using the Default subscribed S-NSSAI in the subscriber UDM slice profile (Slice 2).	AT Command on UE shows Slice 1 (SD=1) as the configured slice, but after attaching, shows Slice 2 (SD=2). The registration messages show the same circumstance, with the UE requesting registration to Slice 1 and the core accepting registration to Slice 2.
The UE connects successfully to Slice 2	The UE successfully attached.
Overall Test	Success

Conclusions and Next Steps

The 5G Security Test Bed's network slicing phase 2 tests were designed to produce, in a real-world environment, two potential exploits enabled by a theoretical network slicing vulnerability in 5G cores. Both scenarios are niche cases that are extremely difficult to execute in practice, and only one exploit was confirmed to be executable, while the other was mitigated by the network. After the Test Bed shared its findings with 3GPP, the standards body released updated technical standards resolving the vulnerability.

Summary of Test Results

Test Case 1 was designed to replicate the exploit described in the 2021 AdaptiveMobile Security Common Vulnerability Disclosure report to GSMA. The test confirmed that a modified request could be sent from a rogue network function and slice, then shared with other network functions. To do so, the NRF generated a valid token for the shared AMF network function and provided it to the rogue network function. The shared AMF network function responded to the maliciously crafted token and granted the rogue network function access to the network, thus indicating that the vulnerability existed and was exploitable. The Test Bed reported its findings to 3GPP, leading to updated standards resolving the potential issue.

Test Case 2 was designed to test a second exploit and confirm that the network would override an incorrectly provisioned UE by comparing its network slice request to the network slice provisions recorded by the network operator. To do so, the UE was incorrectly provisioned with a Requested NSSAI for Slice 1, but the network overrode it using the default subscribed S-NSSAI in the subscriber UDM slice profile (Slice 2). This forced the UE to connect to the correct Slice 2.

Both tests successfully confirmed the Test Bed's hypotheses: Test Case 1 verified that the network slice identifier vulnerability could be exploited in the hypothetical scenario defined in the AdaptiveMobile report. Test Case 2 confirmed that for the second potential exploit, defined by the 5G Security Test Bed's Technical Advisory Committee, the network's built-in controls prevented the vulnerability from being exploited, and the mis-provisioned UE was redirected to its correct slice.

5G Security Test Bed Strengthened 3GPP Standards

As a result of AdaptiveMobile's Common Vulnerability Disclosure, the 3rd Generation Partnership Project (3GPP) standards body began assessing and addressing the hypothetical vulnerability in new releases, but 3GPP could not create definitive standards until the scenario was validated.

The 5G Security Test Bed's efforts, detailed in this report, were the first time the vulnerability was confirmed on a real-world network. As a result of the Test Bed reporting its findings to the

standards body, 3GPP was able to conclusively validate the vulnerability and add a solution in updated technical standards. 3GPP's Service and System Aspects Working Group 3 (SA3) has since fixed this vulnerability within a Change Request (CR) that was accepted and implemented recently in TS 33.501, *Security architecture and procedures for 5G system*, Release 18, in section 13.4.1.1.2.

Specifically, 3GPP now requires the NF Service Producer to confirm that the NF Service Consumer has authorization to access at least one of the slices the UE is registered to, by cross-checking and verifying that the UE's slice identifiers match the NF Service Producer's slice identifiers listed in the access token.

TS 33.501 added the following language to ensure that with shared NFs, the NF slice identifier is now checked:

> *If applicable (e.g., when the request is for information related to a specific UE), the NF Service Producer may check that the NF Service Consumer is allowed to access (as indicated by the NF Service Producer's NSSAIs in the access token presented by the NF Service Consumer) at least one of the slice(s) that the UE is currently registered to, e.g., by verifying that the UE's allowed NSSAI(s) intersect with the NF Service Producer's NSSAIs in the access token.*

The successful execution of these tests also reflects the 5G Security Test Bed's value as a platform for testing and validating theoretical scenarios in real-world conditions, providing validation of use cases that had previously been discussed only in theory.

Next Steps

As new participants and the diversity of test cases grow, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security. The 5G Security Test Bed is exploring future tests of network function security, false base stations, roaming security, and aspects of 5G cloud security that arise with use of the Network Exposure Function (NEF), the Application Function (AF), and Multi-access Edge Computing (MEC). The Test Bed is also exploring opportunities to test configurations and enhance Open Radio Access Network (Open RAN) security.

For more information, or to participate in the 5G Security Test Bed, please contact Harish Punjabi (hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.

About the 5G Security Test Bed

The 5G Security Test Bed reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The Test Bed's members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, SecureG, Intel, and Syniverse; and academic partners the University of Maryland and Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed has a Technical Advisory Committee (TAC) made up of its members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

The 5G Security Test Bed further works with a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Federal Communications Commission (FCC), among others.

The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications

Real-World Testing

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Real-World Applications

The 5G Security Test Bed's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

- Primary Use Cases: Network Security
  - Protecting Information in Transit
  - Roaming Security
  - Subscriber Privacy
  - Zero Trust Network Security
  - False Base Station Detection and Protection
  - 5G Cloud Network Security

- Secondary Use Cases: Devices and Applications
  - High-Resolution Video Surveillance (e.g. Smart Cities, Large Venues)
  - LTE/5G Drones with High-Resolution Video Feedback (e.g. Smart Cities)
  - Dynamic Supply Chain Verification (Real-Time Monitoring and Logistics)
  - Automated, Reconfigurable Factories
  - Autonomous Vehicles
  - Immersive AR/VR

The 5G standalone network architecture and network slicing capability tested for this report are key components of these applications because they enable service to be customized to diverse needs and requirements. The test cases outlined here show how these new and evolving uses can successfully adopt enhanced security capabilities while improving performance.

Appendix: Acronyms

3GPP	Third Generation Partnership Project
5G STB	5G Security Test Bed
5GS	5G System
AMF	Access & Mobility Management Function
AMS	AdaptiveMobile Security
AT Command	Attention Command
BBU	Baseband Unit
CNOM	Core Network Operations Manager
CP	Control Plane
CSRIC	Communications Security, Reliability, and Interoperability Council
CVD	Common Vulnerability Disclosure
DMC	Dual-Mode Core
DN	Data Network
DNN	Data Network Name
eMBB	Enhanced Mobile Broadband
eNB/eNodeB	Evolved Node B
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
gNB/gNodeB	Next Generation Node B
GSMA	Global System for Mobile Communications Association
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
LTE	Long Term Evolution
mMTC	Massive Machine-Type Communication
MNO	Mobile Network Operator
mTLS	Mutual Transport Layer Security
MTP	Mobile Test Platform
NAS	Non-Access Stratum
NF	Network Function
NIST	National Institute of Standards and Technology
NR	New Radio
NRF	Network Repository Function
NSA	Non-Standalone
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
PCAP	Packet Capture
PCC	Packet Core Controller

PCF	Policy Control Function
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
ppm	Packets per million
RAN	Radio Access Network
RAT	Radio Access Technology
SA	Standalone
SBA	Service-Based Architecture
SD	Slice Differentiator
SDR	Software-Defined Radio
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
TAS	Telecom Application Server
TC	Test Case
TLS	Transport Layer Security
TP	Test Point
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UMD	University of Maryland
UP	User Plane
URI	Uniform Resource Identifier
URLLC	Ultra-Reliable Low-Latency Communication
VNF	Virtualized Network Function
VPN	Virtual Private Network
WG	Working Group

References

[i] 5G Security Test Bed, *Securing 5G: Network Slicing Phase 1 Test Report*, Q1 2023. Available at

[ii] AdaptiveMobile Security, *A Slice in Time: Slicing Security in 5G Core Networks*, March 24, 2021. Available at https://www.enea.com/insights/white-paper-slicing-security-in-5g/

[iii] 3GPP TS 33.501, *Security architecture and procedures for 5G System*, Release 18.

[iv] 3GPP TS 23.501, *System architecture for the 5G System (5GS)*, Release 16.6.0.