FGT5008 Redirection of traffic via user plane network function

Description: An adversary can divert user plane traffic for one or more UEs via a user-plane function, to monitor user data.

Traffic diversion is a threat relating to network elements of the user plane. A compromised or misconfigured NF (as documented in the procedures below: UPF, SMF, …) is used to send or cause to send a command to a user plane (routing) function that results in altering the traffic flow. This threat involves compromising a network element to divert traffic flows and allow a malicious actor to eavesdrop on user traffic.

Redirection attacks on the core network result in not only communication interception, but also in billing discrepancies.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Impact, Collection

Metadata:

* Architecture Segment: User plane
* Platforms: 5G Network
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Rogue or misconfigured SMF | An adversary controlling the SMF can redirect existing uplink UE traffic by sending to UPF a N4 Session Modification Request (or: selecting another UPF- or, by sending to UPF another “Redirect server” [which the adversary controls] in the FAR in the N4 session (“The UPF reports to the SMF whether it supports traffic redirection enforcement in the UPF through the UPFunction Features IE.” [6]) Clause 5.8.2.3.3 of [5]  Similarly, the SMF can send a session modification request to the UPF and redirect UE traffic (downlink) — See clauses 4.4.1.2 & 4.4.1.3 of [4]. |
| Rogue AF or rogue/misconfigured NEF | The “Application Function influence on traffic routing” service is designed for MEC applications for local processing of data traffic in order to reduce latency. However, this capability can be misused by rogue AF or rogue/misconfigured NEF. The traffic redirection occurs after the NEF takes action that affects the UPF behavior. Clause 5.6.7 Table 5.6.7-1 first row “Traffic Description” of [5], clause 4.3.6 of [4]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| M1040 | Monitor internal API calls between NFs for suspicious activities |
| M1047 | Audit insecure NF configurations |
| FGM5019 | Authorize all API calls by external AFs to NEF |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Acquire UPF IP address/control | An adversary must have control of the UPF IP address or a UPF |
| Control SMF/NEF/AF | An adversary must first control the SMF or NEF, or AF |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| Subscriber data | All user plane subscriber data |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Monitor AF to NEF APIs for illegitimate traffic redirection requests. Monitor Nnef\_TrafficInfluence\_Update API calls from AF to NEF for traffic redirection requests to unauthorized DNN & S-NSSAI. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| Subscriber uplink & downlink data intercept | If an adversary redirects to their own server, they can access the uplink and downlink data of the subscriber, who will not be aware that the traffic is being intercepted. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| ENISA “Threat Landscape for 5G Networks Report”, Nov 2019. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks |
| “Bhadra framework”: S.P. Rao, S. Holtmanns, T. Aura, “Threat modeling framework for mobile communication systems” | https://arxiv.org/abs/2005.05110v1 |
| 3GPP TS 23.502 “Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)”. | https://www.3gpp.org/DynaReport/23502.htm |
| 3GPP TS 23.501 “Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS)”. | https://www.3gpp.org/DynaReport/23501.htm |
| UCC 5G UPF Configuration and Administration Guide | https://www.cisco.com/c/en/us/td/docs/wireless/ucc/upf/Ultra-Cloud-Core-5G-UPF-Config-Guide.html |

#doNotParse

References: To be added later when the URL works:

* Positive Technologies, (2020). 5G SA Core Security Research. Previously available at:

https://positive-tech.com/knowledgebase/research/5g-sa-core-security-research/. (now blocked as the company is headquartered in Russia).

But now (Aug 20 2022) I found it cited as part of GSMA: Positive Technologies: 5G security issues, Nov 2019. <https://www.gsma.com/membership/resources/positive-technologies-5g-security-issues/> . However, their redirection hint is in an security of SS7 paper, which I could not find.