FGT5029 Exploit Semi-public Facing Application

Description: Adversary sends specifically crafted messages from an interconnect/interworking partner against roaming interface to gain access to the service function, e.g., SEPP, or to obtain information from the interworking facing service function.

A semi-public application or service is one that is only reachable by an adversary over an interworking network that is typically only exposed to mobile network operators (MNO), internetwork packet exchange providers (IPX), Value Added Services (VAS) providers. An adversary that has previously compromised, through other techniques, another service on the interworking network may be in a position to use this technique against an operator’s interworking facing service interfaces. The adversary does not necessarily need to compromise a roaming partner but needs to be on a network which can reach the target interface.

The technique uses specifically formatted signaling messages to cause unexpected behavior that the adversary has previously determined to permit gaining access to the roaming interface system or network functions reachable via SEPP (N32), AMF/MME (N26), or N3IWF interfaces. The specially crafted messages may also permit the collection of information about the targeted operator and its users. The adversary may target the SEPP itself or place specially crafted messages within legitimately authenticated messages that the SEPP passes to NFs that can result in compromise of the NF or information collection. N9 interfaces and non-3GPP interfaces exposed to interworking partners may also be targeted by adversaries. The Network Function addendum to the ATT&CK technique [T1190]( https://5g-security.pages.mitre.org/techniques/T1190) covers internet facing service interfaces.

Labelling:

* Sub-techniques:
* Applicable Tactics: Initial-Access, Collection

Metadata:

* Architecture Segment: Roaming
* Platforms: SEPP, UPF
* Access type required: N/A
* Data Sources: SEPP network communication logs, SEPP service logs, SEPP access logs, NF logs,
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1050 | Use of a Web Application Firewall may only allow properly formatted service communication. |
| FGM5010 | Redeploy SEPP regularly to prevent dwell time aka use non-persistence |
| M1051 | Aggressive patching may reduce window of vulnerability if a known vulnerability |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Vulnerability Identified | Adversary must have identified a vulnerability susceptible to the specially crafted message that results in an ability to use additional techniques. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SEPP | Security Edge Protection Proxy |
| AMF | Access & Mobility Management Function |
| UPF | User Plane Function |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Monitor application logs for evidence of unexpected access requests or potential pattern of errors logged that might indicate attempts to create unexpected behavior |
| DS0028 | Monitor login session logs for evidence an adversary has created accounts or setup access after compromise of the service via specially formed packets on the service API |
| DS0029 | Observe unusual traffic to the SEPP and any evidence of unusual source or destinations from the SEPP that might indicate a source of specially formed packets. |

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) |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| “5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class,“ TS 33.517 ver. 17.0.0, 3rd Generation Partnership Project (3GPP), Sec. 4.2.3.3-4.4, Jun. 2021 | https://www.3gpp.org/DynaReport/33517.htm |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |
| “Security Edge Protection Proxy (SEPP),” Broadforward, Amersfoort, Netherlands, Accessed: May 17, 2022 | https://www.broadforward.com/security-edge-protection-proxy/ |
| “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes,“ TR 33.926, 3GPP, Sec. 5.3.7.2. | https://www.3gpp.org/DynaReport/33926.htm |

#doNotParse

In prior discussions, the team decided to scope this to all interworking/interconnect facing interfaces including NFs exposed via SEPP. The scope was also to include both access to the NF as well as DoS of the function.

5/31/22 – Discussion between Michaela, Surajit, and Andy concluded that FGHT5029 would be Semi-Public only and cover API DOS and Initial access through a SEPP to an NF. T1199.501 would cover API Integrity and information collection. As a result, T1190.501 is not needed as FGT 5029 includes all of T1190.501 which was DoS of the SEPP via API only. References were merged into this technique

6/7/22 – Discussion with the whole group led to this technique focusing on internetworking network position and not trusted partner position and excludes DoS. DoS is covered in T1499 Addendum and Trusted partner is in T1199.501.

