T1498.501 Flooding of core network components

Description: An adversary may send high volumes of registration signaling to degrade performance or deny access to the network for all UEs.

Upon power on or coming out of flight mode, a UE needs to register with 5G network in order to get services from the network. After it gets connected to the network, UE sends several signaling messages to maintain the connection and to request new services. If any of those signaling messages are sent repeatedly to 5G network, the network spends its resources to process those request messages, which may overwhelm some critical Network Functions (NFs) such as AMF.

A malicious UE sends repeated Attach requests which cause Access and Mobility Function (AMF) to start many registrations. Alternatively, when a load balancing Service Communication Proxy (SCP) is not employed, an adversary in the network sends many otherwise-legitimate control messages to a NF so as to overload it. Network service is degraded for all other users in that area (served by AMF).

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Impact

Metadata:

* Architecture segment: Control-plane, slice
* Platforms: 5G network
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of Concept/Observed: Observed

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 |
| Control plane signaling storm from (at least) one malicious UE | Because network slices and network functions can be shared, malicious UE can create control plane storms.  AMF Message Flooding for a shared slice with shared NFs:  (1) An initial AMF validates if the user (UE) is allowed to access the subscribed S-NSSAI: AMF contacts the UDM to request the UE’s Slice Selection Subscription data. The initial UDM may contact the UDR for the UE's Slice Selection Subscription data, then provides the data to the AMF.  (2) During the t0 to t-delta time interval that it takes to perform (1), the UE drops the initial AMF then re-attaches to the AMF, restarting the validation.  (3) The UE recursively performs (2), which recursively performs (1), creating a "UE-AMF-UDM-UDR-AMF" message storm sandwiched in between an "Attach-Detach" storm.  (4) Since this is a shared slice with shared NFs, the control plane storm (Attach-UE-AMF-UDM-UDR-AMF-Detach-Attach-recursively repeat) creates a DoS condition. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5498 | Employ a firewall or other rate control box on the N2 interface [from RAN to AMF]  (May not be available in the market). Employ a NAS-MM (Non-access stratum Mobility Mgmt) application layer proxy at the edge of the network, having the capability to limit UE request rate.  In addition, SCP can act as load balancer between the service consumer (AMF) and service producer (UDM). (Annex E of [2]) |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
|  |  |

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. |
| Network services (AMF) | AMF functionality serving the UEs should be available. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0018 | Application layer DoS attack detection mechanism can be used to detect repeated attempt of UE attach-detach cycle within a short period.  NAS-MM (Non-access stratum Mobility Mgmt) app layer proxy with UE request rate limiting capability. |

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) |
| AMF service will not be available to legitimate users during attack. | If AMF services are down, all services for the existing UEs which use NAS layer will not be available. For example: mobility, session management (QoS etc.), PDU session set up / tear down, SMS over NAS, location management. [Section 8.2.2.1 of [2] |

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 |
| 3GPP TS 23.501: System architecture for the 5G System (5GS) | https://www.3gpp.org/DynaReport/23501.htm |

#doNotParse

Background info: NAS-MM (Mobility Mgmt) level rate limiting

F5 application layer load balancer and reverse proxy can mitigate signaling storms directed to core NFs.

<https://www.f5.com/pdf/solution-guides/overcoming-4g-to-5g-migration-challenges-overview.pdf>