FGT1587.004 Develop Capabilities: Exploits

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: An adversary may develop exploits that target the UE to execute malicious code. The adversary may identify a vulnerability in the UE modem and exploit this to execute malicious code[1]( https://keenlab.tencent.com/zh/whitepapers/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-on-5G-Smartphones-wp.pdf). The adversary may need specific knowledge of the modems used in specific UEs and exploits might be viable for specific models of UEs or the class of UE utilizing a specific version of firmware. Vulnerabilities may be discovered in multiple ways and exploiting the vulnerability may require previous use of techniques to obtain an operator RAN position or deploy a false base station that the UE would utilize. Vulnerabilities on the AT interface may be potentially discovered through dynamic analysis or fuzzing[2]( https://dl.acm.org/doi/pdf/10.1145/3416125).

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: Resource Development

Metadata:

* Architecture Segment: UE
* Platform(s): 5G, 4G, 3G
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of concept/Observed: Proof-of-Concept

Procedure Examples

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

Mitigations

|  |  |
| --- | --- |
| **MID** | **Use** |
| M1001 | Install security updates for known vulnerabilities |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromise of base station | Adversary may need to compromise a base station to exploit the UE |
| False base station | Adversary may need to deploye and get UE to connect to adversary controlled base station. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Base Station |  |

Detection

|  |  |
| --- | --- |
| **DSID** | **Detects** |
|  |  |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| M.Grassi and X. Chen, “Over The Air Baseband Exploit: Gaining Remote  Code Execution on 5G Smartphones, Retrieved May 16, 2023 | https://keenlab.tencent.com/zh/whitepapers/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-on-5G-Smartphones-wp.pdf |
| I.Karim, F.Cicala, et.al.,“ATFuzzer: Dynamic Analysis Framework of AT Interface  for Android Smartphones,” Retrieved May 16, 2023 | https://dl.acm.org/doi/pdf/10.1145/3416125 |

#doNotParse