FGT5006.001 DNS Manipulation: Layer 2 Redirection of Encrypted DNS

Description: An adversary using a fake gNB and fake UE device can manipulate encrypted traffic to achieve plaintext manipulation of DNS requests sent by the victim UE to the network over the radio interface.

Adversary can modify DNS requests UE sent over the air, even though they are encrypted, if it knows the correct DNS address and there is no integrity protection on user plane data. User plane integrity protections prevent this attack on typical 5G RAN links, however these protections are optional. Alternatively, an adversary may have bid-down the UE as a precondition to achieve the effect.

Labelling:

* Sub-Technique(s): N/A
* Applicable Tactics: Initial Access, Persistence

Metadata:

* Architecture segment: User plane
* Platforms: 5G
* Access type required: user
* Data Sources: Network Traffic
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary employs the aLTEr procedure | In this active attack named ALTER, adversary exploits the fact that LTE user data is encrypted in counter mode (AES-CTR) but not integrity protected, which allows an adversary to modify the message payload. This is applicable in 5G when the user data integrity algorithm is set to NULL. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM1557 | Use strong data integrity protection algorithms |
| M1020 | Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unauthenticated DNS Services | The end user must not have the capability to validate whether it is communicating with a malicious DNS or a valid one. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| DNS Servers | Whoever controls the DNS Servers controls how and what end users connect to over the network, making DNS Servers a type of critical infrastructure. |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0029 | Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP) |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| DNS control | Adversary has redirected the end user to their own DNS system and can now conduct adversary-in-the-middle attacks. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| D. Rupprecht, K. Kohls, T. Holtz, and C. Popper, “Breaking LTE on Layer Two” https://alter-attack.net | https://alter-attack.net/media/breaking\_lte\_on\_layer\_two.pdf |