FGT5009 Weaken Integrity

Description: An adversary may compromise a network device’s integrity capability or configuration in order to exploit the non-integrity protected data communication.

Integrity can be used to protect transmitted data traffic against unauthorized changes. Algorithms for user data and signaling communication take a plaintext or encrypted message and compute, using a symmetric secret key, a keyed MIC (message integrity check) or MAC (Message Authentication Code). A recipient in possession of that symmetric integrity key can verify that the message was not modified in transit.

An adversary may alter network signaling or compromise an NF, proxy or gNB that controls the choice of integrity algorithm, so as to enable the weak or no integrity algorithm, thus allowing for manipulation or spoofing of user data or signaling (over the radio interface or within the core network, e.g. Non-SBI, or SBI, or roaming interfaces).

Labelling:

* Sub-technique(s): FGT5009.001, FGT5009.002
* Applicable Tactics: Defense-evasion

Metadata:

* Architecture Segment: RAN, User-plane, Control-plane
* Platforms: 5G
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Weaken integrity over radio interface | An adversary may manipulate gNB signaling to enable NULL integrity over the radio interface (Uu) |
| Weaken integrity within the RAN to core connections | An adversary may change network configuration so that IPSec is not enabled between gNB and UPF (N3) or between gNB and AMF (N2). |
| Weaken integrity within RAN | An adversary may change network configuration so that IPSec is not enabled between two gNBs (Xn). |
| Weaken integrity within SBI | An adversary may disable TLS between two NFs or between one or more NFs and the Service Communication Proxy (SCP) if deployed by MNO. |
| Weaken integrity on the roaming/interconnect | An adversary may disable or weaken integrity protection of the communications between SEPPs (N32 which uses JWS for example) or between visited PLMN UPF and home PLMN UPF (N9).  An adversary may weaken integrity protection on N26 interface between MME and AMF. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1047 | Monitor periodically if integrity protection algorithm is enabled |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary controlling end point | Adversary gets hold of an end point such as gNB to manipulate signaling |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subscriber data | Subscriber signaling and user plane data |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0029 | Data sent over the network or radio interface can be analyzed to check for the integrity algorithm. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subscriber data session impact | Subscriber data session does not get setup (DoS attack) or gets interrupted, spoofed or redirected during an active session. |

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 |

#doNotParse

Background info: Integrity can be used to protect transmitted data traffic against unauthorized changes. Algorithms take a plaintext or encrypted message and compute, using a symmetric secret key, a keyed MIC (message integrity check) or MAC (Message Authentication Code); alternatively, a digital signature can be computed using a private key. A recipient in possession of that symmetric integrity key can verify that the message was not modified in transit; for the digital signature case, a recipient aware of the public key of the sender can verify that the message was not modified in transit.

Adversaries can compromise and manipulate devices that apply integrity to data or signaling traffic, or that configure what algorithms to use for integrity protection, so that weak or no integrity is used. This poses a risk of unauthorized tampering of data and may help facilitate data manipulation.