FGT5018.002 Radio access hardware

Description: An adversary uses unrestricted access to exploit, damage, or destroy Radio Access hardware that lack adequate security.

The use of small-cell antennas requires hardware to be placed in highly accessible locations, such as, commercial and residential buildings, ground-level structures, and existing street furniture (bus stops, info kiosks, and billboards). These solutions count on sharing site spaces in existing infrastructure to reduce costs due to the increased amount of hardware required to maintain Quality of Service (QoS).

Labelling:

* Sub-techniques: N/A.
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: PHYS & Env
* Platforms: Radio access hardware
* Access type required: Physical
* Data Sources: Incident and event monitoring
* Theoretical/Proof of concept/Observed: Theoretical

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 |
| Physical sabotage/vandalism of the network infrastructure | Classified as a deliberate physical attack, this threat relates to actions taken by actors aimed at destroying, disabling or stealing physical assets supporting the 5G Network. A physical attack to 5G critical assets may disrupt, interfere and ultimately cause unavailability of the network service. Despite the existence of physical protection mechanisms (e.g., physical surveillance and surveillance cameras, security locks, security guards), physical breaches and insider threat attacks may still occur. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5005 | Sites should be provided with a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against vandalism. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Improper physical security of radio access hardware | Despite the virtualized structure of the 5G network and all involved network functions, there will be a strong dependency on the physical infrastructure, especially in the initial migration/hybrid 5G deployments. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Radio access hardware (gNB) | RAN-CU & DU, C-RAN MEC and mmWave equipment |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0040 | Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider-level monitoring mechanisms. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Service unavailability | Destruction or damage of these assets may cause unavailability of resources |
| Information destruction | Destruction or damage of these assets may cause information destruction |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, page 202, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| El-Shorbagy, A.-moniem. “5G Technology and the Future of Architecture”. Procedia Computer Science, (2021), volume 182, p121–131. | https://doi.org/10.1016/j.procs.2021.02.017 |