FGT5002 Bypass home routing

Description: An adversary positioned in an operator network may send an SMS delivery location query that will bypass the SMS home router of another operator, allowing the adversary to get the location of the user device.

SMS home routing bypassing is a technique that exploits incorrect implementation or configuration. An adversary sends an SMS delivery location query that does not get intercepted by the SMS home router, so it receives a response by providing the location of the adversary’s target UE.

This technique is applicable to 3G, 4G, and 5G, since 5G systems still need to interconnect with SS7 networks. 5G supports both SMS over IP and SMS over NAS. The routes for SMS are still from SMSC (Short Message Service Center) to STP (Signaling Transfer Point) to either IP-SM-GW (IP Short Message Gateway) for SMS over IP or SMSF (SMS Function) for SMS over NAS. Refer to section 7.2 of [3].

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Defense-Evasion

Metadata:

* Architecture Segment: Control plane
* Platform(s): 5G
* Access type required: N/A
* Data Sources: Logs of external signals received for location queries
* 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 |
| Send SMS location query via SS7 or Diameter | Incorrect implementation/configuration or compromised home SMS router can allow bypass of the SMS location query messages. Deployed SMS router as in Section 7.2.2 of [3] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5004 | Correctly configure SS7 firewall in home network. [4] |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Compromised SMS Center or STP | Access to a host that could pass as belonging to a different operator (roaming partner) |
| Get target user’s phone number | Access to the MSISDN of the user device |

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. |
| UE location | Coarse location: In the form of routing info (MSC address) |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Logs of externally received messages requesting location of user or, logs of outgoing responses to such messages can detect anomalies. Logs are on the NF or functions which interface SMS home router such as MAP IWF or SMSC. See Figure 27 of [3]. |
|  |  |

Post-Conditions

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

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |
| European Union Agency for Cybersecurity (ENISA), “Signaling security in telecom SS7/Diameter/5G”, March 2018 | https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g |
| GSM Association, “Official Document NG.111 - SMS Evolution”, v2.0, Nov. 2020 | https://www.gsma.com/newsroom/wp-content/uploads//NG.111-v2.0.pdf |
| Kirill Puzankov: “Hidden Agendas: bypassing GSMA recommendations on SS7 networks,”accessed on May 25, 2023 | <https://docplayer.net/136483279-Hidden-agendas-bypassing-gsma-recommendations-on-ss7-networks-kirill-puzankov.html> |

#doNotParse

Background info:

SMS delivery from one operator (where the originator UE is currently in) to another (where the destination UE is currently in) may use an unauthenticated SMS delivery location query (“Send-Routing-Info-for-SM-Request Message”). To protect against this possible abuse of location privacy, operators deploy "SMS home routers" which intercept such externally sourced location queries, responding that they will deliver the SMS to the destination subscriber wherever they may be.

GSMA NG.111 Figure 27 shows the exact location of SMS router/firewall where home routing will be implemented.

Diagram, waterfall chart

Description automatically generated

The following figure shows two distinct paths used in 5G: 1) for SMS over NAS via control plane and 2) for SMS over IP via user plane.

Diagram

Description automatically generated