FGT5017 Call Detail Record (CDR) collection

Description: An adversary may query CDR databases in the mobile network to collect communications metadata.

An adversary may compromise the N40 interface between CHF and SMF/SMSF in order to get detailed communication data. An adversary may collect CDRs from mobile networks by using malware.

*Note*: In earlier generations of 3GPP networks, CDRs are generated on switches, and then moved to billing servers.

Labelling:

* Sub-techniques: None
* Applicable Tactics: collection, discovery

Metadata:

* Architecture segment: Control-plane
* Platforms: 5G
* Access Type Required:
* Data Sources:
* 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 |
| Attack on CDR database | Malware “interacts with CDR databases” (possibly from the SMSC, which this malware infects). Data miner is loaded by installation script. The script collects CDR s for certain IMSIs/SUPI, the info therein is voice call metadata, i.e. time, duration, phone numbers. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5101 | Isolate CDR databases from the rest of the IT systems/NOC resources |
| M1043 | CDR database admin users periodically re-checked |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| SMSC is compromised | Rogue or misconfigured SMSC |

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. |
| Subscriber data | Confidentiality of sensitive subscriber data in the form of (calls/data/SMS). |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5012 | CDR databases should log and raise alarms for any suspicious activity: new connections set up, privilege escalation in admin user. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| Leakage of subscriber data | Exposure of subscriber sensitive information such as call/data/text. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| Techradar.com news article Dec. 31, 2020, "T-Mobile data breach sees phone numbers and call records leaked online", Retrieved March 4, 2022 | https://www.techradar.com/news/t-mobile-data-breach-sees-phone-numbers-and-call-records-leaked-online |
| Leong, R, Perez, D. and Dean, T.: “MESSAGETAP: Who’s Reading Your Text Messages” FireEye. 31 Oct 2019 | https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages |

#doNotParse

N40 interface between SMF and CHF.

<https://github.com/emanuelfreitas/3gpp-documentation>

Diagram

Description automatically generated