PTA Security Advisory-No:43

20-March-2019

Threat Classification: SS7 and Diameter Vulnerabilities

Overview: Mobile phones subscribers and operators are exposed to a number of security vulnerabilities associated with SS7 attacks. Exploitation of these vulnerabilities threatens the privacy of the subscriber, availability of services and the income of the operators.

Classification: The GSM Association's (GSMA) Fraud and Security Group has classified SS7 vulnerabilities into three categories based on the general method used to exploit the network:

- **Category 1:** Relies on SS7 packets, which are usually intended to be sent within the network of one operator to collect information from other networks. Attacks using such packets include the ability to track subscribers at street level.

- **Category 2:** Relies on SS7 packets, usually sent between the roamers home network and the networks in which they are actively moving. Exploiting these allows an attacker to manipulate the subscriber's information, for example, bypassing the charging system and intercepting calls.

- **Category 3:** Relies on SS7 packets that are sent between the operator's networks as part of subscriber movement between networks, SMS interworking, and CAMEL operations. Among other things, vulnerabilities in this category allow an attacker to intercept SMS and voice calls.

Exploited Vulnerabilities: Attackers may perform following illegitimate actions by exploiting SS7 vulnerabilities:

- **Call interception:** A malicious attacker can intercept and record calls from a subscriber, without the subscriber or operator's knowledge.

- **Geo-Location:** A malicious attacker can locate the cell phone of a subscriber, knowing only their phone number, with an accuracy of a few meters.

- **Toll fraud:** A malicious attacker can purchase retail subscriptions from an operator, and make outbound toll calls without being charged for these calls. This can cause a significant loss to the operator within a short amount of time when premium numbers are being targeted.

- **Denial of service attack:** A malicious attacker can bring down mobile services for a specific subscriber, a group of subscribers, random subscribers, or in some cases, for the entire network.

- **Wholesale SMS fraud**: A malicious attacker can use a mobile operator's network to terminate or relay large amounts of wholesale SMS messages. SMS firewalls can be deployed to counter, but malicious attackers can bypass some of the first generation firewalls.

Recommendations:

It is strongly recommended to adopt the following standards for Compliance w.r.t above aforementioned context:

- **FS.07 SS7 and SIGTRAN Network Security**
- **FS 11 SS7 Filtering & Monitoring**
- **FS.19 Diameter Interconnect Security**
- **IR.77 Inter-Operator IP Backbone Security Requirements**
- **IR.82 (SS7) – GSMA Interconnection Security**