Security Advisory 2019-020

Simjacker Vulnerability Impacting up to 1 Billion Phone Users

September 16, 2019 — v1.1

TLP:WHITE

History:

- *13/09/2019 — v1.0 – Initial publication*
- *16/09/2019 — v1.1 – Added information about potential impact*

Summary

AdaptiveMobile Security have uncovered a new and previously undetected vulnerability and associated exploits, called Simjacker [1]. This vulnerability is currently being actively exploited. The main **Simjacker** attack involves an SMS containing a specific type of spyware-like code being sent to a mobile phone, which then instructs the SIM Card within the phone to *take over* the mobile phone to retrieve and perform sensitive commands. During the attack, the user is completely unaware that they received the attack, that information was retrieved, and that it was successfully exfiltrated.

Technical Details

According to [2], the attack begins when a SMS – *Attack Message* – is sent to the targeted handset. It can be sent from another handset, a GSM Modem, or a SMS-sending account connected to an A2P account. The message contains a series of SIM Toolkit (STK) instructions, and is specifically crafted to be passed on to the UICC/eUICC (SIM Card) within the device. In order for these instructions to work, the attack exploits the presence of a particular piece of software, called the **S@T Browser** – that is on the UICC. Once the *Attack Message* is received by the UICC, it uses the S@T Browser library as an execution environment on the UICC, where it can trigger logic on the handset.

For the main attack observed, the Simjacker code running on the UICC requests location and specific device information (the IMEI) from the handset. Once this information is retrieved, it can be sent to a recipient number via another SMS (the *Data Message*), again by triggering logic on the handset.

According to the researchers who identified this vulnerability, they were able to make targeted handsets open up web browsers, ring other phones, send text messages, etc. [2]. These attacks could be used for:

- mis-information (e.g., by sending SMS/MMS messages with attacker controlled content),

- fraud (e.g., by dialing premium rate numbers, stealing 2FA tokens sent by SMS),
- espionage (location tracking, but also as a listening device, by ringing a number),
- malware spreading (by forcing a browser to open a web page with malware)
- denial of service (e.g by disabling the SIM card)
- etc.

Products Affected

Many of possible attacks seems to work independent of handset types, as the vulnerability is dependent on the software on the UICC and not the device itself. Devices from nearly every manufacturer are being successfully targeted to retrieve location: Apple, ZTE, Motorola, Samsung, Google, Huawei, and even IoT devices with SIM cards [2].

Up to potentially 1 billion of devices may be impacted [1].

Recommendations

Unfortunately, there is nothing that phone users can do to mitigate the attack. Organizations should contact their mobile operators for specific mitigations and solutions.

The recommendations for the mobile community to deal with the immediate threat is for mobile operators to analyse and block suspicious messages that contain S@T Browser commands [3]. Mobile Operators could also try to change the security settings of UICCs remotely, or even uninstall and stop using the S@T Browser technology completely, but this may be slower and considerably more difficult to do.

References

[1] https://simjacker.com

[2] https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile

[2] https://simalliance.org/wp-content/uploads/2019/08/Security-guidelines-for-S@T-Push-v1.pdf