**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250081-r2**

Online, Electronic meeting, 13 -16 January 2025

**Source: Ericsson**

**Title: New Key Issue on Amplification of resource exhaustion by exploiting AIoT paging messages**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This document proposes to add a new key issue about exploiting paging messages in AIoT in TR 33.713***

# 2 References

# 3 Rationale

Paging of AIoT devices have different properties than paging of regular UEs. Therefore, it is important to study the differences, find related threats and identify potential security requirements.

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 5.X Key issue #X: Amplification of resource exhaustion by exploiting AIoT paging messages

### 5.X.1 Key issue details

. In AIoT, one single paging message coming from the reader/network can be used to trigger multiple devices to respond by using, for example, a mask/filter based on target device identification, or by a group ID of the target devices. Once the target devices are triggered, the reader, core network of the MNO, and the associated AF participate in various steps to accomplish the intended tasks, e.g., inventory reporting and command executing. Unlike regular paging, AIoT paging can happen for devices that are not necessarily already registered in the core network and hence cannot share a session security context with the network.

The paging message can include information that the devices, core network, and MNO can use in successful accomplishment of these tasks in those steps. Therefore, if parts of or the whole paging message is corrupted, the core network of the MNO and the AF can end up wasting computational resources that leads to no successful accomplishment of the intended tasks. Moreover, the corrupted paging message results in waste of radio resources being used by AIoT over the air interface as well.

The above can be used by an adversary that intentionally corrupt the paging message in a way so that many legitimate AIoT devices are triggered by the corrupted paging message, but later, in the core network of the MNO or in the AF, the responses from the AIoT devices are found invalid. This happens not because the devices computed wrong responses, but because the devices used corrupted paging message in computing their responses. Such an attack can cause the MNO and the AF wasting computational resources. It also causes the AIoT reader wasting radio resources that can adversely impact the regular UEs in the same network.

If devices respond to a corrupted paging message, that should be identified as early as possible, and the responses should not be forwarded any further to the core network or to the AF.

### 5.X.2 Security threats

An adversary can cause the core network of an MNO or the AF wasting computational resources by corrupting or spoofing one single paging message, which is surprisingly little work on the adversary’s behalf, that triggers a lot of devices to send a paging response to the legitimate reader.

The above attack can also cause the AIoT reader and serving NG-RAN node wasting radio resources that can adversely impact the regular UEs in the same network.

### 5.X.3 Potential security requirements

Editor’s Note: whether the security threats shall be mitigated through non-standard implementation methods is FFS.

**\*\*\*\*** END OF CHANGE **\*\*\*\***