**3GPP TSG-SA3 Meeting #124 S3-253508**

**Wuhan, China, 13 – 17 October 2025**

**Source: Ericsson**

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

**Document for: Approval**

**Agenda item: 5.2.11**

**Spec: 3GPP TR 33.714**

**Version: 0.0.0**

**Work Item: FS\_AIoT\_SEC\_Ph2**

**Comments**

The amplification of resource exhaustion by exploiting AIoT paging messages was not addressed in Rel-19, see NOTE 2 in clause 5.2.2 of TS 33.369:

*" NOTE 2: While a legitimate network is performing an inventory operation, an attacker may cause amplification of resource exhaustion at the legitimate network side by sending AIoT paging messages for all devices or to a large group of devices, which causes large number of devices sending D2R messages to the legitimate network that the legitimate network does not expect to receive. The security measure to such amplification of resource exhaustion attack is not specified in present document."*

The motivation for not addressing the attack was that Rel-19 AIoT specifications are for isolated private networks only. Since Rel-20 extends the scope to public networks, the amplification of resource exhaustion by exploiting AIoT paging messages should be considered in Rel-20 instead.

\* \* \* First Change \* \* \* \*

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

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

### 5.X.1 Key issue details

Paging of AIoT devices is different than "regular" paging of regular UEs. 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 PLMN, 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 and core network of the PLMN 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 PLMN 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 PLMN 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 PLMN 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 a PLMNor 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.1 Potential security requirements

Editor’s Note: Potential security requirements are FFS

\* \* \* End of Changes \* \* \* \*