Silicon Labs Security Advisory

A-00000447

Subject: Security Advisory for Zigbee protocol and Implementation vulnerabilities – Don't Kick over the Beehive

CVSS Severity: Medium

Base Score: 6.5, Medium
Temporal Score: 6.5, Medium
Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:X/RC:C

Impacted Products:

- All Zigbee-capable SoCs and associated modules, running Ember ZNet 7.1.x or earlier which is delivered as part of GSDK 4.1.x or earlier, may be impacted.
    - EFR32-based and EM35x-based SoCs and associated modules

Technical Summary:

- Researchers at the University of Texas at Dallas have disclosed five vulnerabilities, summarized in the table below, to the Connectivity Standards Alliance (CSA)

Attack #	Description	Type of Attack	Impact
1	**Communication Interruption** Sending ZCL messages with certain cluster IDs causes some devices to stop responding.	Denial-of-Service	Availability
2	**Disconnection** Sending certain NWK or APS messages causes some devices to leave the network.	Denial-of-Service	Availability
3	**Key leakage** Secure rejoin requests with the well-known link key causes the network key to be leaked.	Denial-of-Service	Availability, Confidentiality, Integrity
4	**Integrity Check** Sending NWK messages with an invalid MIC cuses some devices to leave the network.	Denial-of-Service	Availability
5	**Truncated Packet** Sending packets with a truncated network header causes a delayed response in some devices.	Denial-of-Service	Availability

- The researcher's report is available at the following link https://dl.acm.org/doi/pdf/10.1145/3548606.3560703
- Silicon Labs has attempted to confirm these vulnerabilities with the information contained in the paper. At the time of this writing, we have been unable to reproduce these results using Gecko SDK v4.2.0.

Fix/Work Around:

- Mitigations are described in the table below:

Attack #	Recommended Mitigation	Explanation
1	None	This is a classic denial-of-service, like selective jamming. No known method is available for mitigating this type of attack.
2	See note below	Silicon Labs has been unable to reproduce this attack in Ember ZNet 7.2.0, so this version or higher is recommended.
3	Use TrustCenterLinkKey instead of well-known Link key	Rejoining an existing network with the well-known link key leads to the network key being leaked.
4	See note below	Silicon Labs has been unable to reproduce this attack in Ember ZNet 7.2.0, so this version or higher is recommended.
5	See note below	Silicon Labs has been unable to reproduce this attack in Ember ZNet 7.2.0, so this version or higher is recommended.

- Affected users should upgrade to EmberZNet v7.2.0 (distributed with GSDK v4.2.0) or later.

  1. In Simplicity Studio's Help menu, select the 'Update Software' menu item to open the Installation Manager
  2. Click the 'Manage installed packages' button
  3. Select the 'SDKs' tab and find the 'Gecko SDK – 32-bit and Wireless MCUs' section
  4. If there are not currently any Installations, click the 'Install New' button. If there is an SDK already installed, click on the '…' button next to its version number
  5. Click 'Change Version'
  6. In the 'Versions:' dropdown menu, select the desired version
  7. Click 'FINISH'

Guidelines on our security vulnerability policy can be found at https://www.silabs.com/security
For Silicon Labs Technical Support visit: https://www.silabs.com/support