Security Advisory (SA-2023-234)

Security Advisory ID:	SA-2023-234-v1_1	**Advisory Initial Release:**	2023-05-10
Classification:	Public	**Advisory Updated:**	2023-07-06
		Embargo until:	2023-07-01
Title:	Unauthorized Thread Network Key Update		
CVE IDs	CVE-2023-2626		
Affected products:	**Product**	**Version**	
Hardware	nRF52811	All build codes	
	nRF52833	All build codes	
	nRF52840	All build codes	
	nRF5340	All build codes	
	Thingy:53	All build codes	
Software	nRF5 SDK for Thread & Zigbee	4.2.0 and earlier	
	nRF Connect SDK	2.4.0 and earlier	
	Thread Border Router Reference	A892bf7 -> docker image and earlier	
		A892bf7 -> source recommendation	
	Thread Certification Reference Dongle	20230119-ce1647697 and earlier for Thread 1.3	
		20221027-d5a53efde and earlier for Thread 1.2	
		20200818 and earlier for Thread 1.1	
	Thread Certification Reference Border Router	1.3-20230119 + 20230119-ce1647697 and earlier for Thread 1.3	
		20221027+20221027-d5a53efde and earlier for Thread 1.2	
	Thingy:53 pre-compiled firmware – Matter and HomeKit	2023-03-24 release and earlier	

Overview

This Security Advisory addresses a vulnerability impacting devices using OpenThread implementation of Thread specification. The vulnerability allows an attacker to compromise the entire Thread network.

At the time of publishing there is no known exploitation of this vulnerability in the market.

Nordic Semiconductor is cooperating with Thread Group and our partners to resolve and communicate this vulnerability to impacted customers on a Confidential basis prior to public disclosure of the vulnerability on 2023-07-01.

Reference:

- Thread Group Confidential - OpenThread KeyID Mode 2 Security Vulnerability (Updated: 27th April 2023) https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=4252
- https://github.com/openthread/openthread/security/advisories/GHSA-vr3r-363g-72j9

CVE ID	CVE-2023-2626	**CVSS 3.1**	**Base Score:**	7.6 High
			Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Description

This vulnerability impacts all Thread devices using OpenThread and allows an attacker in physical proximity to compromise non-router-capable devices and the entire Thread network in the case of router-capable devices.

The vulnerability allows an attacker in physical proximity to inject arbitrary IPv6 packets into the Thread network via IEEE 802.15.4 frame transmissions. Because the Thread Management Framework (TMF) protocol does not have any additional layer of security, the attacker could exploit this vulnerability to update the Thread Network Key and gain full access to the Thread network.

There is no known exploitation of vulnerability.

Affected customers

All customers implementing Thread using OpenThread stack provided in an affected software version.

Security Risk

Application layers typically have their own end-to-end security. As a result, such application layers maintain confidentiality and integrity even with the OpenThread vulnerability. However, an attacker can still affect availability by preventing delivery of Thread messages.

Resolution

A patched precompiled OpenThread binary is available on request for the following SDK releases:

- nRF Connect SDK v2.0.2
- nRF Connect SDK v2.2.0
- nRF Connect SDK v2.3.0
- nRF5 SDK for Thread and Zigbee v4.1.2
- nRF5 SDK for Thread and Zigbee v4.2.0

The patched OpenThread binaries listed above have been certified to enable Thread re-certification by Inheritance for customers using them.

nRF Connect SDK

The vulnerability is patched in public nRF Connect SDK version 2.4.1. It is mandatory to use this or later release of nRF Connect SDK for all future development.

nRF5 SDK for Thread and Zigbee:

nRF5 SDK for Thread and Zigbee is deprecated. A patched release of nRF5 SDK for Thread and Zigbee will not be provided.

In addition, updates will be provided for development tools

Thread development tools:

- Thread Border Router Reference
  - From source - patched in public nRF Connect SDK version 2.4.1
  - As Docker image – patched in public nRF Connect SDK version 2.4.1
- Thread Certification Reference – firmware released to Thread Group in May 2023 both Dongle and Border Router

Pre-compiled firmware in nRF Programmer for Thingy:53 mobile application:

- Matter Weather Station – vulnerability patched together with release of nRF Connect SDK version 2.4.1.
- HomeKit Weather Station – vulnerability patched together with release of nRF Connect SDK version 2.4.1.

Change Log

2023-05-10 – v1.0: Initial Confidential release to Thread Group Member companies

2023-07-06 – v1.1: Updated for Public release

Acknowledgement

Nordic PSIRT would like to thank Thread Group for prompt notification of the vulnerability.

Technical contact at Nordic Semiconductor:

If you have questions or concerns regarding this Security Advisory remediating actions, open a Private Support Case at:

https://devzone.nordicsemi.com

Commercial contact at Nordic Semiconductor:

Contact your existing Regional Sales Manager, if you do not have an existing relationship send us a message and they will contact you :

https://www.nordicsemi.com/About-us/Contact-Us

Report a product security vulnerability:

https://www.nordicsemi.com/About-us/PSIRT

Product Security at Nordic Semiconductor

Nordic Semiconductor is committed to providing hardware, software and services which enable the development of secure end-products. Secure development and vulnerability management processes are put in place to try to ensure products are secure-by-design and that security is maintained throughout their lifecycle. However, we acknowledge that no level of security can guarantee that products will resist all forms of attacks. Our documentation is provided to enable customers to make their own assessment of the products suitability for their end-product use-case. Each customer must determine if the security provided by the hardware, software and services is appropriate for their application and to their satisfaction.

Our Product Security Incident Response process supports the evaluation, communication and resolution of potential vulnerabilities discovered in our hardware, software, and services. In the case of a vulnerability being discovered in our deployed products, Nordic endeavors to communicate with affected customers in a timely manner to facilitate coordinated vulnerability disclosure.

This document, suggested mitigations, and any security features of Nordic products are provided on an “AS IS” basis without warranty of any kind. Nordic disclaims all express and implied warranties. Under no circumstance shall Nordic be liable for any damages whatsoever, including direct, indirect, incidental, consequential, or special damages related to or arising from this document or its content.