# Security advisory TN1436-ST-PSIRT: potential bypassing of Bluetooth® Low Energy Secure Connection authentication

## Overview

This document describes the security advisory related to the potential bypassing of Bluetooth® Low Energy Secure Connections authentication. The affected products are listed in Table 1.

## Affected products

**Table 1. Affected products**

| Part number | Embedded software |
|---|---|
| BlueNRG-1, BlueNRG-2 | STSW-BLUENRG1-DK from version 2.1.0 to 3.2.2 |
| BLUENRG-2N | STSW-BNRG2N-V320 and V330 |
| BlueNRG-LP, BlueNRG-LPS | STSW-BNRGLP-DK from 1.0.0 to 1.2.0 |
| STM32WB Series microcontrollers | STM32CubeWB version 1.14.1 and earlier |

The evaluation boards using any of the foregoing products are also affected.

## How to verify that the product is affected

In all the products listed above, the vulnerability is present only if Bluetooth® Low Energy Secure Connections (SC) is used for authentication, and the application has not initialized a random value for Out of band (OOB) pairing during the initialization of the Bluetooth® Low Energy stack.

## Description of the potential vulnerability

An attacker device can coerce the affected product into successfully completing an OOB SC pairing, passing the two SC authentication stages, even without receiving any negotiated OOB data from the affected product itself. This results in the authentication of the attacker, thus providing unauthorized access to data requiring authentication.

## Impact

When an attacker is within the Bluetooth® Low Energy range of an affected product, and the attacker has appropriate tools specially programmed to execute this attack, an unexpected access to the information protected by the Bluetooth® Low Energy Secure Connections authentication may occur.

## Remediation/mitigation

After each initialization of the Bluetooth® Low Energy stack, call the `aci_gap_set_oob_data()` command to pass the random value to be used later during OOB pairing. The random value must be generated with 128 bits of entropy.

The steps are summarized in the following code example. The `hci_le_rand()` command is used to generate the random value. However any other source of entropy can be used instead, provided it conforms to the requirements of Bluetooth® Low Energy Core Specifications [Vol 2] Part H, Section 2.

```
uint8_t status, address[6] = {0,}, random[16];
status = hci_le_rand( random );
if ( status )
    system_error( );
status = hci_le_rand( random + 8 );
if ( status )
    system_error( );
status = aci_gap_set_oob_data( 0, 0, address, 1, 16, random );
if ( status )
    system_error( );
```

**Credit**

Purdue University and Pennsylvania State University.

**Contact information**

psirt@st.com

## Revision history

Table 2. **Document revision history**

| Date | Revision | Changes |
|---|---|---|
| 30-Nov-2022 | 1 | Initial release. |
| 13-Dec-2022 | 2 | Changed document scope to public. |

**IMPORTANT NOTICE – READ CAREFULLY**

The STMicroelectronics group of companies (ST) places a high value on product security, and strives to continuously improve its products. However, no level of security certification and/or built-in security measures can guarantee that ST products are resistant to all forms of attack including, for example, against advanced attacks which have not been tested for, against new or unidentified forms of attack, or against any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software which are used by a customer to create their end product or application. As such, regardless of the incorporated security features and/or any information or support that may be provided by ST, each customer is responsible for determining if the level of security protection in and ST product meets their needs, both in relation to the ST product alone and when incorporated into a customer end product or application.

Security advisories (including suggested mitigations), and security features of ST products (inclusive of any hardware, software, documentation, and the like), together with any enhanced security features added by ST and any technical assistance and/or recommendations provided by ST, are provided on an "AS IS" BASIS. AS SUCH, TO THE EXTENT PERMITTED BY APPLICABLE LAW, ST DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, unless the applicable written and signed contract terms specifically provide otherwise.

ST reserves the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Customer should obtain the latest relevant information on ST products before placing orders.

Customers are solely responsible for the choice, selection, and use of ST products, and ST assumes no liability for application assistance or the design of customers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.