STBLEMesh Android application and STSW-BNRG-Mesh solution: potential reflection and replay risk in certain authentication modes

Overview:

This security advisory describes a potential risk related to reflection and replay scenarios during provisioning or authentication when certain authentication modes are used in:

1. The STBLEMesh Android application,
2. The STSW-BNRG-Mesh software solution,
3. Custom applications developed using the BlueNRG-Mesh Android SDK.

The risk may arise in specific configurations and usage scenarios.

Affected products:

Product	Version	Type	Note
STBLEMesh Android application	STBLEMesh V1.17 and below versions	Android application	-
STSW-BNRG-Mesh	1.13.001 and below versions	Software solution for BLE Mesh	-
BlueNRG-Mesh Android SDK	1.15.000 and below versions	Software SDK	BlueNRG-Mesh Android SDK is part of STSW-BNRG-Mesh

STBLEMesh Android application:

- Open the side menu and navigate to “About”.
- If the version number is 1.17 or below, the application may be affected.

Custom Android applications built with BlueNRG-Mesh Android SDK:

- Check the release notes of the BlueNRG-Mesh SDK used to build the application.
- If the SDK version is 1.15 or below, the application may be affected.

Description:

In certain authentication modes, reflection and replay scenarios may arise during the provisioning and authentication process. The described scenarios are associated with provisioning interactions and may require proximity and active participation in the provisioning process.

In some circumstances, these scenarios could affect the intended authentication behavior, including assumptions regarding proof of knowledge of the AuthValue.

For more details, refer to the Bluetooth SIG guidance:

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/impersonation-mesh/

Note: The URL belongs to a third-party. It might be moved, modified, and/or inactivated by them at any time. STMicroelectronics is not responsible for the content of the referenced website.

Impact:

If exploited under certain conditions, this risk could affect provisioning or authentication behavior and may allow an unauthorized party to obtain the NetKey and join the mesh network.

Remediation:

1. For users of the STBLEMesh Android application from Google play:
   – Update to version 1.18 or later, which includes updates intended to mitigate the risk described in this advisory.
2. For developers using STSW-BNRG-Mesh (BlueNRG-Mesh Android SDK):
   – Rebuild and release applications using STSW-BNRG-Mesh version 1.14 or later, the corresponding BlueNRG-Mesh Android SDK version is 1.16.000 or later.
3. If an immediate update is not feasible:
   – Consider restricting use of the following authentication modes in affected deployments where possible:
      ◦ No OOB
      ◦ Static OOB

Credit:

Matt Emerick

Contact information:

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
09-Jun-2026	1	Initial release.

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") place a high value on product security, and strive 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, advanced attacks that have not been tested, new or unidentified forms of attack, or any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software that are used by the purchasers 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, the purchasers are responsible for determining whether the level of security protection in an ST product meets their needs, both in relation to the ST product alone and when incorporated into the purchasers' end product or application.

ST technical notes, security bulletins, security advisories, and the like (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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

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

If the purchasers identify an ST product that meets their functional and performance requirements, but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

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.