HMS Security Advisory

Anybus Wireless Bluetooth Low Energy Pairing
HMSSAR-2023-05-02-001

<table>
<thead>
<tr>
<th>Version</th>
<th>Summary of changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial release</td>
<td>May 2, 2023</td>
</tr>
</tbody>
</table>

Overview

Bluetooth® Low Energy Pairing in Bluetooth Core Specification v4.0 through v5.3 may permit an unauthenticated MITM to acquire credentials with two pairing devices via adjacent access when the MITM negotiates Legacy Passkey Pairing with the pairing Initiator and Secure Connections Passkey Pairing with the pairing Responder and brute forces the Passkey entered by the user into the Initiator. The MITM attacker can use the identified Passkey value to complete authentication with the Responder via Bluetooth pairing method confusion.

All Anybus Wireless Bridge II and Anybus Wireless Bolt products are affected per definition of the Bluetooth® Core specification.

The exploitability score is very low at 1.2/10. The Attack Complexity is high (hard to utilize the vulnerability), the attacker must be adjacent to the network and the attacker must interact with the devices to make use of vulnerability. The vulnerability only affects specific device setups:

- The device that Anybus Wireless Bridge II/Bolt is pairing with is a device that supports LE Secure Connections
- At least one of the pairing devices must support Passkey entry (the other may support either entry or display of a Passkey)

The above listed device setup should be treated as unauthenticated, thus being open to Man-In-The-Middle attacks the same way as other unauthenticated pairing methods.

Affected products and versions

- Anybus Wireless Bridge II (Articles AWB300X, AWB301X, AWB31XX, AWB33XX) – All firmware versions
- Anybus Wireless Bolt (Articles AWB200X, AWB203X, AWB240X) – All firmware versions
- Anybus Wireless Bolt Serial (Articles AWB201X) – All firmware versions
- Anybus Wireless Bolt CAN (Articles AWB202X) – All firmware versions
- Anybus Wireless Bolt Starterkit (Articles AWB230X, AWB240X) – All firmware versions

Severity / CVSS Score


Recommendations

HMS recommends that Bluetooth® LE is disabled if it is not in use.

1 CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

HMS Networks
https://www.hms-networks.com/cybersecurity
If Bluetooth® LE is needed, the Anybus Wireless Bridge II/Bolt should only be connectable and discoverable during the pairing phase. Only enable connectable and discoverable when they are needed.

**Product updates**

No firmware update will be released to fix this issue.

**Acknowledgements**

HMS thanks Ingo Suleck from WAGO for finding and notifying about the vulnerability in a controlled way.

**Additional information**