WPA2 Key Reinstallation Vulnerabilities in ABB TropOS wireless mesh products

ABBVU-PGGA-1KHW028907

Initial Release: October 27, 2017 (Revision 1)

Update Date: January 4, 2018 (Revision 2 – remedial firmware release information added)

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

All TropOS broadband mesh routers and bridges operating on Mesh OS release 8.5.2 or prior.

Vulnerability ID

ABB ID: ABBVU-PGGA-1KHW028907

CVE IDs: CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake

CVE-2017-13078: reinstallation of the group key in the Four-way handshake

CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

CVE-2017-13080: reinstallation of the group key in the Group Key handshake

CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake

CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake

CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

Summary

ABB is aware of reports of vulnerabilities in the product versions listed above.

An attacker who successfully exploited this vulnerability could decrypt, replay, and forge some frames on a WPA2 encrypted network.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake

CVSS v2 Base Score: 5.4

CVSS v2 Vector and Link: *AV:A/AC:M/Au:N/C:P/I:P/A:P*

CVSS v3 Base Score: 6.8

CVSS v3 Vector and Link: *AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N*

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13077

CVE-2017-13078: reinstallation of the group key in the Four-way handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13078

CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13079

CVE-2017-13080: reinstallation of the group key in the Group Key handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13080

CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13081

CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13082

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13084

CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13086

CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13087

CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2017-13088

Corrective Action or Resolution

ABB has completed investigating this vulnerability in order to provide adequate protection to customers. The problem is corrected in the following product versions:

Product	Firmware Release
All TropOS broadband mesh routers and bridges operating on Mesh OS release 8.5.2 or prior.	Mesh OS release 8.5.3.

ABB customers with a current Complete Software Care or Complete Software + Hardware Care subscription are advised to contact ABB Wireless support on phone +1(408) 331 6800, ext. 4, or email tropos.support@nam.abb.com.

Vulnerability Details

An industry-wide vulnerability exists in the WPA2 key management algorithm included in the product versions listed above. The vulnerability may allow an attacker to decrypt, replay, and forge some frames on a WPA2 encrypted network.

TropOS routers with Wi-Fi client access enabled and using WPA2 are vulnerable as hosts/authenticators on the Wi-Fi interface(s).

TropOS 1410 bridges (a discontinued class of products) connecting upstream over WiFi and using WPA2 are vulnerable as supplicants on the upstream Wi-Fi interface.

Mitigating Factors

The TropOS mesh wireless interfaces are not vulnerable.

Wired client interfaces (Ethernet, Serial) are not vulnerable.

An attacker must be in physical proximity of the WiFi access point and connected client to be successful.

If the communication across the Wi-Fi link is encrypted at Layer 3, e.g. SSH, SSL, HTTPS or SNMPv3 encrypted, privacy is maintained during an otherwise successful attack.

Workarounds

If possible, encrypt communication across the Wi-Fi link at Layer 3 using e.g. SSH, SSL, HTTPS or SNMPv3.

There is no complete workaround which allows protected Wi-Fi access to the TropOS Mesh.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could decrypt, replay, and forge some frames on a WPA2 encrypted network

What causes the vulnerability?

An industry-wide vulnerability exists in the WPA2 key management algorithm included in the product versions listed above. The vulnerability may allow an attacker to decrypt, replay, and forge some frames on a WPA2 encrypted network.

What is the affected product or component?

TropOS routers with Wi-Fi client access enabled and using WPA2 are vulnerable as hosts/authenticators on the Wi-Fi interface(s).

TropOS 1410 bridges (a discontinued class of products) connecting upstream over WiFi and using WPA2 are vulnerable as supplicants on the upstream Wi-Fi interface.

What might an attacker use the vulnerability to do?

An attacker who successfully exploits this vulnerability will target the four-way authentication “handshake” performed when a Wi-Fi client device connects to the protected TropOS Wi-Fi network. The encryption key can be resent multiple times, and if attackers collect and replay those retransmissions in particular ways, the Wi-Fi Layer 2 encryption can be compromised.

How could an attacker exploit the vulnerability?

Once Layer 2 encryption is compromised, the attacker can exploit the vulnerability by eavesdropping and manipulating traffic sent across that Wi-Fi connection that is not protected by higher layer security. This would require that the attacker is physically located near the client and the TropOS mesh router.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to be in the direct proximity of a vulnerable client and/or TropOS mesh router.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Support

ABB Wireless customers are advised to contact ABB Wireless support on phone +1(408) 331 6800, ext. 4, or email tropos.support@nam.abb.com.

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.