ABB DOC ID: 9AKK107992A3688
REVISION: D
DATE: 2021-07-02

CYBER SECURITY ADVISORY

ControlTouch serial number can be misused to access customer configuration

ABBVU-ABBVREP0044-9AKK107992A3688

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

This vulnerability belongs to the product Busch®-ControlTouch and how it connects to the Busch-Jaeger- and ABB-Cloud for Building Automation. The vulnerable part locates in the subdomain:

1.) https://controltouch.my.busch-jaeger.de/register, version: prior to 2021-05-03 and

2.) https://controltouch.eu.mybuildings.abb.com/register, version: prior to 2021-05-03

Please note: Because the vulnerability originates in the cloud Software, it is independent from Busch-Jaeger- or ABB-branded devices.

Vulnerability ID

ABB ID:	ABBVREP0044
CVE ID:	CVE-2021-22272

Summary

ABB is aware of a privately reported vulnerability in the ControlTouch cloud subsystem. The cloud subsystem is updated to remove the vulnerability.

An attacker who successfully exploited this vulnerability could modify the configuration of the ControlTouch of an authorized user.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) 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.

CVSS v3 Base Score:	6.5
CVSS v3 Temporal Score:	6.2
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:H/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:H/RL:O/RC:C
NVD Summary Link:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22272

Recommended immediate actions

After investigating the vulnerability ABB has updated the cloud subsystem to fully resolve the vulnerable part. On end user side no action is required in terms of updating the system. However, in case a successful attacker got control over an installed ControlTouch, the authorized end user should take action to remove the unauthorized access. Please follow the instructions in section: Vulnerability Details.

Vulnerability Details

A vulnerability existed in the cloud subsystem, see Affected Products. Even thought the vulnerability has been fixed, the following explains how to determine if an end user is affected or not.

The vulnerability origins in the commissioning process where an attacker of the ControlTouch can enter a serial number in a specific way to transfer the device virtually into her/his my.busch-jaeger.de or mybuildings.abb.com profile. A successful attacker can observe and control a ControlTouch remotely under very specific circumstances.

Determining if a customer is not affected

You or your customer is NOT affected if ONE of the following questions can be answered with YES (correct):

Question	YES (correct) / NO (not correct)
Is the ControlTouch-device NOT connected to the Internet?	
Are you or your customer paying a monthly fee for using the ABB or Busch-Jaeger remote service?	
Is the ControlTouch-device visible under "My Home" within your (or your customers) my.busch-jaeger.de or mybuildings.abb.com account?	
Check if all local users are known to you? How to check: - Open your my.busch-jaeger.de or myBuildings.abb.com account - Please go to "My Installations" - Please open your device(s) - If you start in the Wizard mode, then please enter the advanced mode by pushing the button "Go to advanced mode" - Open in the top the part "devices" - Select the part "Local users" - Now please check if you see only local users which should have access to your ControlTouch. - Are these "local users" that you can see now, are known?	

If you answered all of this 4 questions with "NO", please contact your Busch-Jaeger Sales support at: info@de.bje.de

Please note:

Still, this is no evidence that the ControlTouch is actively in control of an unauthorized user. It only indicates that this might be the case.

Legal Notice:
The above information 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 above information, and assumes no responsibility for any errors that may appear. 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 araising from the use of this information, or from the use of any hardware or software described in this information, even if ABB or its suppliers have been advised of the possibility of such damages.

How this vulnerability has been fixed

The serial number of a ControlTouch can now only be entered once after purchasing it. In accordance to the commissioning process, this is done by the Installer prior to further configuration of the device.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could observe and control a ControlTouch installed on premise of a building or apartment remotely.

What causes the vulnerability?

The vulnerability was caused by a step in the commissioning process where an attacker could enter the serial number on a registration page in a certain time frame. Since the vulnerability has been fixed, new exploitations are not possible anymore. Existing exploitations may still exist. Therefore, this advisory explains how end-users find out if they are affected or not. See also Vulnerability Details.

What is the affected product or component?

Please see section: Affected Products

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could observe and/or control a building like the authorized end-user could do.

How could an attacker exploit the vulnerability?

A successful attacker could login to a ControlTouch device with role: end-user.

Could the vulnerability be exploited remotely?

Yes, a successful attacker was able to control a ControlTouch device just as an authorized end-user.

What does the update do?

The vulnerability could be fixed by updating the cloud subsystem. The update is deployed since 2021-05-03.

See also section: How this vulnerability has been fixed

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

No, ABB received information about this vulnerability through responsible disclosure.

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.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

M. Sc. Tobias Mengel of Technische Hochschule Köln for finding this vulnerability, providing a detailed description and professional cooperation.

Prof. Dr.-Ing. Luigi Lo Iacono of Hochschule Bonn-Rhein-Sieg for support and professional cooperation.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

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