ABB DOC ID: 9AKK107992A6475
REVISION: -
DATE: 2021-08-13

CYBER SECURITY ADVISORY

free@home System Access Point FW integrity check can be bypassed.

ABBVREP_R9057

Notice

Affected Products

Affected products are listed in Table 1 List of affected products. Firmware Versions affected are Version 2.6.3 and earlier.

ABB Product Id	Title
2CKA006200A0156	System Access Point 2.0 US
2CKA006200A0155	System Access Point 2.0 (ABB)
2CKA006220A0240	System Access Point 127V (ABB)
2CKA006220A0136	System Access Point (ABB)
2CKA006220A0031	System Access Point (BJE)
2CKA006200A0130	WL-System Access Point 127V (ABB)
2CKA006200A0105	WL-System Access Point (ABB)
2CKA006200A0154	System Access Point 2.0 (BJE)
2CKA006200A0071	WL-System Access Point (ABB)

Table 1 List of affected products

Vulnerability ID

ABB ID: ABBVREP_R9057

CVE ID: CVE-2021-22276

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An update is available that resolves a publicly reported vulnerability in the product versions listed above. The resolving firmware version is: 2.6.4 and newer.

An attacker who successfully exploited this vulnerability could downgrade the devices firmware to any older version or can install an unauthorized SW change.

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: 6.1

CVSS v3 Temporal Score: 5.7

CVSS v3 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H/E:F/RL:O/RC:C

CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H/E:F/RL:O/RC:C

Recommended immediate actions

Customers using one or more of the products listed in section: Affected Products are requested to update to the latest firmware version available.

ABB recommends that customers apply the update at the earliest convenience.

Vulnerability Details

A vulnerability exists in all variants of the free@home System Access Point (see section Affected Products for a complete list) firmware Version 2.6.3 and earlier. The successuful attacker can modify an existing FW image and bypass the integrity check of the System Access Point.

Version 2.6.4 and newer resolves this problem by adding additional integrity checks.

The vulnerability can only be exploited if the attacker has access to the local Network in which the System Access Point is installed. A user interaction is required to actually trigger the update after the FW is uploaded by the attacker.

Automatic updates, where the System Access Point is triggered by the user to download a new FW from ABB/Busch-Jaeger update Server, will work as intended as the connection is secured via TLS and version 2.6.4 and later, and will add additional checksum files securing the integrity of the overall folder structure inside the update-image-archive-file.

Please make sure the System Accesspoint is connected to the Internet and that it can download the latest FW from the ABB/Busch-Jaeger update server. To make sure that you have installed the latest FW version, please enable the autoupdate feature and reboot the System Access Point. Finaly install the FW downloaded in the previous step.

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.

Mitigating Factors

In case it is not possible to update the System Access Point FW to version 2.6.4 or later, the following mitigations prevent an exploitation of the vulnerability reported in this document:

- Ensure to only allow updating the System Access Point FW via the automatic update method where the device downloads the latest FW automatically from an ABB/Busch-Jaeger server.
- Do not allow downgrading to an older FW version than the one installed on the System Access Point.
- Ensure your local network is protected against attacks using recommended Industry best practices. Please consult the manual of your firewall or network router for advises how to harden it appropriately.

Frequently Asked Questions

What is the scope of the vulnerability?

The successful attacker can modify an existing FW image and bypass the integrity check of the System Access Point.

What causes the vulnerability?

An attacker who successfully exploited this vulnerability can downgrade the installed FW to an older version and/or modify an existing FW.

What is the System Access Point?

The System Access Point is the central unit of the BUSCH-FREE@HOME® Eco-System. See section Affected Products for a list of product-HW and -SW known to be affected.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could install older FW versions which might contain other vulnerabilities that appear useful to the attacker. Furthermore, the successful attacker may modify an existing FW with functionality in favor of his/her attack plans.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by modifying an existing FW image bypassing the integrity check of the System Access Point. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that (s)he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, according to the system handbook (please see https://busch-jaeger-catalogue.com/), the operation of the System Access Point must be protected by an appropriate firewall or NAT-router with no port forwarding or similar method, that allows to connect to it from the Internet.

An attacker can only upload malicious FW to the System Access Point if (s)he has access to the local network where the device is connected to. For the installation of the FW, the legitimate user needs to trigger the installation after a successful FW upload prior to the authentication.

What does the update do?

The update removes the vulnerability by modifying the way that the System Access Point does the integrity check before installing a new FW version.

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

Yes, ABB became aware of a published report explaining how to downgrade the FW of a System Access Point.

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. It is assumed that the vulnerability was exploited by a developer who intended to learn more about the insights of his/her own System Access Point. We have not been informed about any attack from a 3rd party to a legitimate users installation.

Acknowledgements

The finder of the Vulnerability preferred to keep this report anonymously. We respect this decision and thank her/him anyways.

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.