DOCUMENT ID: 2PAA122974
REVISION: B
DATE: 2021-09-09

CYBER SECURITY ADVISORY

SECURITY - ABB Base Software for SoftControl Remote Code Execution vulnerability

CVE ID: CVE-2020-24672

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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations (e.g. ICS-CERT).

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

ABB Base Software for SoftControl, all versions up to and including System Version 6.1.

Vulnerability IDs and Product Issue Numbers (PIN)

CVE ID	Product Issue Number*
CVE-2020-24672	800xACON-AD-5110-00208

* Product Issue Number - is an ABB internal unique identifier to identify an issue. The Product Issue Number is for example used to identify the correction of a problem in a Release Note.

Summary

ABB is aware of a vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could via the network insert and run arbitrary code in a computer running the affected product.

Recommended immediate actions

ABB recommends updating to a corrected version released for the product in this advisory. Customers unable to install the update are advised to review the Mitigations and Workarounds section for additional advice on how to reduce the risk associated with these vulnerabilities.

The vulnerability has been corrected in System 800xA 6.1.1 with the introduction of signed application downloads to the SoftController.

Vulnerability severity and details

A vulnerability exists in the product versions listed above. An unauthenticated attacker could exploit the vulnerability by sending a specially crafted message to a computer runnning the affected product and by this insert and run arbitrary code in that computer. The code will run with the privileges of the user that launched the SoftController.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2020-24672 - Remote Code Execution vulnerability

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:	9.8 (Critical)
CVSS v3 Temporal Score:	8.8 (High)
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/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:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-24672

Mitigating factors

The SoftController is normally started on request by the logged in user. The vulnerability is not present when the SoftController is not running. Customers are recommended to launch it only when it is needed.

When a project has been downloaded to the SoftController, it will not accept a generic message that could exploit the vulnerability. An attacker would need to create specific attack messages. Customers are recommended to launch the SoftController just before downloading to it.

A way to limit the impact of such an exploit is to run the SoftController in an environment with limited resources and limited connections to more critical systems. As few other functions as possible should be used in the same computer. If the SoftController is run in a virtual machine in a virtualization environment, the amount of other resources that could be accessed can be limited.

The system function `InhibitDownload(Inhibit)` can be used to prevent download to the SoftController. Calling this function from application code in the SoftController with `Inhibit` set to True will inhibit the download possibility. This can be controlled via a communication variable to get an Access Enable function.

[1] 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.

Workarounds

The SoftController can be configured using the Control Builder running in the same computer or in a separate computer. By default, TCP port 102 is opened for communication from other computers.
If the SoftController and the Control Builder are run in the same computer, the SoftController only needs to be able to communicate locally, so for this usage, a way to avoid network-based exploitation of this vulnerability is to close TCP port 102 in the Windows firewall.

If the SoftController is intended to be accessed from the network TCP port 102 cannot be closed. In such cases the network should be protected against unauthorized access.

A way to restrict network access, to allow only a controlled set of computers to connect to the Soft Controller, is to use IPSec. For usage together with System 800xA this is described in in the user manuals “System 800xA 5.1 IPsec Configuration Tool” (2PAA107224-510) and “System 800xA 6.1 Post Installation” (2PAA111693-600 and 2PAA111693-610).

If IPSec cannot be used, an alternate method is to use the Windows Firewall to control what computers that are able to connect to the SoftController e.g. by limit the IP addresses allowed to connect to TCP port 102.

Frequently asked questions

What is the scope of the vulnerability?

An unauthenticated attacker who successfully exploited this vulnerability could insert and run arbitrary code in a computer running the SoftController.

What causes the vulnerability?

The vulnerability is caused by lack of access control and of input data validation in the SoftController.

What is the SoftController?

The Soft Controller is a test and debugging tool used for basic program testing during engineering. It is also used for 800xA Simulator and APC.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could insert and run arbitrary code in an affected computer.

Can functional safety be affected by an exploit of this vulnerability?

The Soft Controller is not certified for use in safety control, thus cannot affect functional safety of the plant.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to a computer running the SoftController. This would require that the attacker has access to the same network as the affected computer, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that the attacker installs malicious software on a node on this network. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an unauthenticated attacker who has network access to an affected system node could exploit this vulnerability.

Is there a corrected version of the SoftController?

A correction is available in System 800xA 6.1.1.

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.

General security recommendations

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

- Place control systems in a dedicated control network containing control systems only.
- Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.
- If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.
- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

More information on recommended practices can be found in the following documents:
3BSE080520* - System 800xA Secure Deployment Guide

Acknowledgement

ABB thanks Flavian Dola of AIRBUS for helping to identify the vulnerabilities and protecting our customers.

References

3BSE041880* - System 800xA, AC 800M - Getting Started

3BSE035980* - System 800xA, AC 800M - Configuration

2PAA107224-510 System 800xA 5.1 IPsec Configuration Tool

2PAA111693* - System 800xA 6.x Post Installation

Support

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

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2021-06-23

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
B	Recommended actions and FAQ	Update with the 800xA 6.1.1 being released	2021-09-08
	Vulnerability severity	Updated Temporal Score.	