ABB DOC ID: 2PAA121236
REVISION: B
DATE: 2020-04-17

CYBER SECURITY ADVISORY

SECURITY Inter process communication vulnerability in System 800xA

CVE ID: CVE-2020-8478, CVE-2020-8484, CVE-2020-8485, CVE-2020-8486, CVE-2020-8487, CVE-2020-8488, CVE-2020-8489

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.

© Copyright 2020 ABB. All rights reserved.

Affected Products

OPC Server for AC 800M	all versions
MMS Server for AC 800M	all versions
Base Software for SoftControl	all versions
800xA for DCI	all versions
800xA for MOD 300	all versions
800xA RNRP	all versions
ABB System 800xA Base	all versions
800xA Batch Management	all versions
800xA Information Management	all versions

Vulnerability IDs and Product Issue Numbers

CVE ID	Product Issue Numbers *	Product
CVE-2020-8478	800xACON-OL-5020-00164	OPC Server for AC 800M, MMS Server for AC 800M, Base Software for SoftControl
CVE-2020-8484	800xADCI-OL-6100-007	800xA for DCI
CVE-2020-8485	800xAMOD-OL-6100-007	800xA for MOD 300
CVE-2020-8486	800xARNR-OL-3110-00001	800xA RNRP
CVE-2020-8487	800xASYS-OL-5120-00213	ABB System 800xA Base
CVE-2020-8488	800xAPMB-OL-6030-035	800xA Batch Management
CVE-2020-8489	800xAINM-OL-6030-002	800xA Information Management

* 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 public reports of a vulnerability in the product versions listed above. There is a potential risk of local denial-of-service or tampering attack on the System 800xA nodes.

An attacker who successfully exploited this vulnerability could make the system node inaccessible or tamper with runtime data in the system.

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'

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

OPC Server for AC 800M, MMS server for AC 800M, Base Software for SoftControl

CVSS v3 Base Score: 5.3 (Medium)

CVSS v3 Temporal Score: 5.2 (Medium)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8478

800xA for DCI

CVSS v3 Base Score: 7.8 (High)

CVSS v3 Temporal Score: 7.6 (High)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8484

800xA for MOD 300

CVSS v3 Base Score: 7.8 (High)

CVSS v3 Temporal Score: 7.6 (High)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8485

800xA RNRP

CVSS v3 Base Score: 6.6 (Medium)

CVSS v3 Temporal Score: 6.5 (Medium)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8486

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

ABB System 800xA Base

CVSS v3 Base Score: 6.6 (Medium)

CVSS v3 Temporal Score: 6.5 (Medium)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8487

800xA Batch Management

CVSS v3 Base Score: 7.8 (High)

CVSS v3 Temporal Score: 7.6 (High)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8488

800xA Information Management

CVSS v3 Base Score: 7.8 (High)

CVSS v3 Temporal Score: 7.6 (High)

CVSS v3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8489

Recommended immediate actions

ABB recommends changing any user account passwords which are suspected to be known by an unauthorized person. Interactive logon (both local and remote) is recommended to be disabled for the service account.

Please note that the vulnerability can only be exploited by authenticated users, so customers are recommended to ensure that only authorized persons have access to user accounts in System 800xA.

The vulnerability is planned to be corrected in future product versions.

This advisory will be updated when the corrected versions are released, or otherwise relevant information becomes available.

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

Vulnerability Details

The above mentioned products consists of several Windows processes running on each system node. Some of these processes in the products are vulnerable when performing inter-process communication to exchange data. An attacker could exploit the vulnerability by injecting garbage data or specially crafted data. Depending on the data injected each process might be affected differently. The process could crash or cause communication issues on the affected node, effectivly causing a denial-of-service attack. The attacker could tamper with the data transmitted, causing the product to store wrong information or act on wrong data or display wrong information.

For an attack to be successful, the attacker must have local access to a node in the system and be able to start a specially crafted application that distrupts the communication.

OPC Server for AC 800M, MMS server for AC 800M, Base Software for SoftControl
An attacker who successfully exploited the vulnerability would be able to affect the online view of runtime data shown in Control Builder.

800xA for DCI, 800xA for MOD 300
An attacker who successfully exploited the vulnerability would be able to manipulate the data in such way as allowing reads and writes to the controllers or cause windows processes for 800xA for DCI and 800xA for MOD 300 to crash.

ABB System 800xA Base, 800xA RNRP
An attacker who successfully exploited the vulnerability would be able to affect node redundancy handling. The attacked node could perceive other nodes to be unavailable, which will disrupt the communication. When running the system in simulation mode, the simulated clock could be affected.

800xA Batch Management
An attacker who successfully exploited the vulnerability would be able to affect how the UI is updated during batch execution. The compare and printing functionality in batch could also be affected.

800xA Information Management
An attacker who successfully exploited the vulnerability would be able to affect the runtime values that are to be stored in the archive. Also, can make Information Management history services unavailable to the clients.

Mitigating Factors

As described above, the mitigating factor is that an attacker needs to be able to login to an account in the system and to execute specially crafted software, so the primary mitigation is to ensure that only authorized persons have access to user accounts on the system nodes. This also includes any user accounts accessing the system via remote tools like Remote Desktop. Additionally, introduction of new software in the system should only be performed by authorized administrators.

This attack may also be mitigated by application whitelisting. Please contact ABB for information about how to use application whitelisting on System 800xA.

More information on recommended practices can be found in section References.

Workarounds

There are no workarounds for this vulnerability, only mitigating actions. The products require an update to fully remedy the vulnerability.

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could cause a local denial-of-service on the affected system node or to read and write data to/from MOD 300 controllers or DCI controllers.

What causes the vulnerability?

The vulnerability is caused by weak access control settings for objects used to exchange information between System 800xA processes on the same machine.

What is the OPC Server for AC 800M?

The OPC Server exposes an OPC interface against clients for accessing runtime data, alarms and events from the AC 800M controllers. The user selects which AC 800M controllers the OPC Server shall be connected to.

What is MMS Server for AC 800M?

The MMS Service is used for communication between Control Builder, OPC Server, Soft Controller and Loop Check Controller.

What is the Base Software for SoftControl?

The Soft Controller is a controller used for testing 1131 applications during engineering.

What is the System 800xA for DCI?

800xA for DCI provides connectivity between the DCI Harmony Distributed Control Unit (HDCU) controllers and the 800xA System.

What is the System 800xA for MOD 300?

800xA for MOD 300 provides the connectivity to the MOD 300 Controller family along with specific MOD 300 displays working in the 800xA operating environment.

What does the affected components in ABB System 800xA Base do?

The affected components in ABB System 800xA Base provides applications with run-time critical information for clients to be able to connect and communicate with system services. It also provides a simulated time when running the system in simulation mode (which requires admin users membership to enter).

What is the 800xA Batch Management?

800xA Batch Management is an application software package for configuring, scheduling, and managing batch operations.

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

What is the 800xA Information Management?

800xA Information Management provides intelligent data access functions to both real-time and historical information from all applications in the extended automation system. This allows all levels of personnel to make quick, informed decisions, and take the appropriate actions to improving efficiency and profitability.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible or could manipulate with the data transmitted between processes. For more details, see section Vulnerability Details.

Can functional safety be affected by an exploit of any of these vulnerabilities?

No, exploits of these vulnerabilities cannot affect the integrity of any safety function in System 800xA.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted application that disturbs the inter-process communication. When running this application on a system node it could cause one or several System 800xA processes to crash or behave unexpectedly.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access and access to an account that can login to the system node remotely could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed. See *Mitigating factors*.

Is there an update that corrects the problem?

ABB is currently investigating corrections to the problem.

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 William Knowles at Applied Risk for helping to identify the vulnerabilities and protecting our customers.

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.

References

3BSE080520* System 800xA, Security Deployment Guide.

3BSE041389* System 800xA, Engineering Planning and Concepts.

3BSE034463* System 800xA Network Configuration.

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.

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-03-30
B	P7	Added FAQ question on functional safety	2020-04-16

© COPYRIGHT 2020 ABB. ALL RIGHTS RESERVED.