CYBERSECURITY ADVISORY

SECURITY System 800xA Weak File Permissions

CVE ID: CVE-2020-8472, CVE-2020-8473

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

OPC Server for AC 800M	versions 6.0 and earlier
Control Builder M Professional	versions 6.1 and earlier
MMS Server for AC 800M	versions 6.1 and earlier
Base Software for SoftControl	versions 6.1 and earlier
ABB System 800xA Base	versions 6.1 and earlier

Vulnerability IDs, Product Issue Numbers

CVE ID	Product Issue Numbers	Product
CVE-2020-8472	800xACON-MS-4100-001	OPC Server for AC 800M Control Builder M Professional MMS Server for AC 800M Base Software for SoftControl
CVE-2020-8473	800xASYS-OL-5120-00195 800xASYS-OL-5120-00196	ABB System System 800xA Base

Summary

ABB is aware that the product versions listed above contain vulnerabilities which require user attention.

Windows folders, used by system functions in System 800xA, allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploited the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.

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 pro-vided 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.

OPC Server for AC 800M

CVSS v3 Base Score:	5.5 (Medium)
CVSS v3 Temporal Score:	5.4 (Medium)
CVSS v3 Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:H/RL:W/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:N/I:N/A:H/E:H/RL:W/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE 2020-8472

Control Builder M Professional, MMS Server for AC 800M and Base Software for SoftControl

CVSS v3 Base Score: 3.3 (Low)

CVSS v3 Temporal Score: 3.3 (Low)

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

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE 2020-8472

ABB System 800xA Base

CVSS v3 Base Score: 7.3 (High)

CVSS v3 Temporal Score: 7.1 (High)

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

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

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8473

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.

The vulnerability in the OPC Server for AC 800M was corrected in System 800xA 6.1, while in the Control Builder M Professional, MMS Server for AC 800M and Base Software for SoftControl and ABB System 800xA Base it will be corrected in future releases of System 800xA. The vulnerability is planned to be corrected in the next release on the 6.0.3 LTS track after 6.0.3.3.

Please note that the vulnerabilities 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.

Vulnerability details

Some folders used for the components and products included in the product versions listed above allow low privileged users to read and modify system files.

OPC Server for AC 800M
An attacker who successfully exploited the vulnerability in the AC 800M OPC Server could prevent the AC 800M OPC Server from automatically reconnect to AC 800M controllers after restart of the OPC server and thus block updates of OPC data to and from AC 800M controllers. This vulnerability itself does however not allow an attacker to force a restart of the OPC server.

Control Builder M Professional, MMS Server for AC 800M and Base Software for SoftControl
An attacker who successfully exploited the vulnerability in the AC 800M Control Builder, MMS Service, Soft Controller, could manipulate log files and enable/disable functions for AC 800M Control Builder, MMS Service, Soft Controller. Enabled/Disabled functions will only have an affect after restart of the AC

800M Control Builder, MMS Service, Soft Controller. This vulnerability itself does however not allow an attacker to force a restart of the Control Builder, MMS Service or Soft Controller.

ABB System 800xA Base
An attacker who successfully exploited the vulnerability in one of the ABB System 800xA Base functions could escalate his/her privileges, execute arbitrary code and affect various engineering functions leading to corrupt applications.

Mitigating factors

As described above, the mitigating factor is that an attacker needs to be able to login to an account in the system, 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.

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

Workarounds

To prevent an attacker from executing arbitrary code Application Whitelisting can be used.

To completely avoid the other risks, the affected products need to be updated.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could escalate his/her privileges, execute arbitrary code, cause system functions to stop and to corrupt user applications.

What causes the vulnerability?

The vulnerability is caused by weak access control lists for folders used by system functions in System 800xA, allowing low privileged users to modify system and application files.

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 the Control Builder M Professional?

The Control Builder is the engineering tool for AC 800M controllers. Configuration is downloaded from the Control Builder to AC 800M controller.

What is the MMS Server for AC 800M?

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

What is the Base Software for SoftControl?

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

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

The affected component in ABB System 800xA Base distributes files between system nodes.

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 and allow the attacker to insert and run arbitrary code.

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 exploit the vulnerability by logging in to an 800xA node and modify the files in the folders with weak access control lists.

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*.

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.

Acknowledgement

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

References

3BSE080520* System 800xA, Security Deployment Guide.

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

3BSE034463* System 800xA Network Configuration.

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 cybersecurity 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	P5 all	Added FAQ question on functional safety Misc clarifications	2020-04-17