DOCUMENT ID : 7PAA000908
REVISION : A
DATE: 2022-01-24

CYBER SECURITY ADVISORY

SECURITY - OPC Server for AC 800M - Remote Code Execution Vulnerability

CVE ID: CVE-2021-22284

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.

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

800xA, Control Software for AC 800M[1]
OPC Server for AC 800M, Version 5.1.0-x, 5.1.1-x, 6.0.0-1 to 6.0.0-3

Control Builder Safe, version 1.x and 2.0 including,
OPC Server for AC 800M, Version 5.1.1-1 and 6.0.0-1

Compact Product Suite - Control and I/O
OPC Server for AC 800M, Version: 5.1.0-x, 5.1.1-x, 6.0.0-x

Vulnerability IDs and Product Issue Numbers (PIN)

CVE ID	Product Issue Number*
CVE-2021-22284	800xACON-OL-5100-00315

* 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 Release Notes.

[1] For reference to corresponding 800xA System Version see table 3 in *3BSE080447 800xA Online Upgrade and Co-existence, Versions Compatibility*.

Summary

ABB is aware that OPC Server for AC 800M contains a Remote Code Execution vulnerability. An authenticated remote user with low privileges who successfully exploited this vulnerability could insert and execute arbitrary code in the node running the AC800M OPC Server.

Recommended immediate actions

ABB advises affected customers to install the updates to address the vulnerability. 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 this vulnerability.

The vulnerability is corrected as follows:

CVE ID	Product	Version
CVE-2021-22284	800xA, Control Software for AC 800M	6.1.0-0 and later, 6.0.0-4 (coming revision)

Customers on version 5.1 or older are recommended to upgrade to a supported version that is not affected by this issue such as version 6.1 or later.

Vulnerability severity and details

A vulnerability exists in the ABB OPC Server for AC 800M included in the product versions listed above. An attacker could exploit the vulnerability by inserting and executing arbitrary code.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[2].

CVE-2021-22284 Remote Code Execution vulnerability

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 v3.1 Base Score: 8.4 (High)

CVSS v3.1 Temporal Score: 7.6 (High)

CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-22284

[2] 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.

Mitigating factors

The vulnerability is related to accessing a COM Interface. So, it is recommended to perform COM/DCOM hardening. This involves turning off DCOM and making sure only valid users can access the OPC Server COM objects locally.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Workarounds

No work arounds exist. Please refer the “Recommended Immediate Actions” Section.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could execute arbitrary code in the node running the AC800M OPC Server.

What causes the vulnerability?

The vulnerability is caused by improper configuration of access control list for COM interfaces.

What is AC800M OPC Server?

The OPC Server for AC 800M is used for reading run-time data and/or alarms and events from controllers via an OPC interface

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could execute arbitrary code.

How could an attacker exploit the vulnerability?

An attacker with low access privileges could exploit the vulnerability by inserting and executing arbitrary code in the affected node. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node 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.

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

No. Functional safety is not affected as OPC Server is Non-SIL.

Is the AC 800M controller affected?

No, neither the HI controllers nor the PA controllers are affected by this issue.

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 documents in References section.

Acknowledgement

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

References

3BSE034463*	System 800xA Reference - Network Configuration
3BSE035983*	AC 800M OPC Server

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	2022-01-20