DOCUMENT ID: 7PAA001499
REVISION: A
DATE: 2022-02-17

CYBER SECURITY ADVISORY

SECURITY - AC 800M MMS - Denial of Service vulnerability in MMS communication

CVE ID: CVE-2021-22277

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

800xA, Control Software for AC 800M
AC 800M Controller Firmware, Version 5.1 all versions, 6.0.0-0 to 6.0.0-3, and 6.1.0-0 to 6.1.1-1.
AC 800M High integrity Controller Firmware, Version 5.1.1-x, 6.0.0-0 to 6.0.0-3, and 6.1.0-1 to 6.1.1-1.

Control Builder Safe, versions 1.x, 2.0 and 3.0 including,
AC 800M High Integrity Controller Firmware, Version 5.1.1-1, 5.1.1-2 CC1, 6.0.0-1, and 6.1.1-0.
AC 800M Controller Firmware, Version 5.1.1-2, 6.0.0-1, and 6.1.1-0.

Compact Product Suite - Control and I/O
AC 800M Controller Firmware, Version: 5.1 all versions , 6.0.0-0 to 6.0.0-3, and 6.1.0-0 to 6.1.1-1.

ABB Base Software for SoftControl
AC 800M SoftController, Version: 5.1 all versions , 6.0.0-0 to 6.0.0-3, and 6.1.0-0 to 6.1.1-1.

Vulnerability IDs and Product Issue Numbers (PIN)

CVE ID	Product Issue Number*	Product
CVE-2021-22277	800xACON-OL-5100-00291	800xA - Control Software for AC 800M, Control Builder Safe, Compact Product Suite - Control and I/O and ABB Base Software for SoftControl

* 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 an issue in Release Notes.

Summary

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

An attacker who successfully exploited this vulnerability in the MMS protocol stack could cause the affected products to be inaccessible for a period of time or stop.

Recommended immediate actions

See mitigating factors. ABB is currently investigating this vulnerability to provide adequate protection to customers.

The issue is currently planned to be corrected in the following product versions. Other product versions may be relevant in future revisions:

CVE ID	Product	Version
CVE-2021-22277	800xA, Control Software for AC 800MCompact (including ABB Base Software for SoftControl)	6.2.0-0 (coming revision), 6.1.1-2 (coming revision), 6.0.0-4 (coming revision)
	Control Builder Safe (including ABB Base Software for SoftControl)	Next version after 3.0
	Compact Product Suite - Control and I/O (including ABB Base Software for SoftControl)	6.2.0-0 (coming revision)

Customers on version 5.1 or older are recommended to upgrade to a supported version that is not affected by this issue

Vulnerability severity and details

A vulnerability exists in the MMS protocol stack in the AC 800M controller firmware included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the affected product to stop or become inaccessible.

Other communication protocols, application code execution and I/O copy is not affected by this vulnerability.

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

CVE-2021-22277 - 800xA, Control Software for AC 800M, Control Builder Safe, Compact Control Builder AC 800M, ABB Base Software for SoftControl

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	7.3 (High)
CVSS v3.1 Vector:	7.3 (High)
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:U/RC:C

[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.

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-22277

Mitigating factors

Following the recommendations in the user documentation and General security recommendations will limit the exposure for unauthorized access.

The Control Network is a trusted network zone that should be protected from unauthorized access. Refer to section “General security recommendations” for further advise on how to keep your system secure.

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, 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, and others that must be evaluated case by case.
Process control & automation systems should not be used for general business functions (e.g. Internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for malicious software before they are connected to a control system.

Workarounds

No workaround exists. Refer to the chapter mitigating factors to limit the exposure for the vulnerability.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could cause the MMS communication in the affected controller to be inaccessible for a period of time (up to 30 seconds). If the communication has not recovered after this time the controller will stop.

What causes the vulnerability?

The vulnerability is caused by lack of input data validation in the MMS protocol stack in the affected products.

What is the MMS protocol stack?

The MMS protocol stack is the software implementation of the MMS communication protocol used by the affected products. The protocol defines communication messages transferred between controllers as well as between the engineering station and controllers.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected AC 800M controller to become inaccessible or stop.

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 an affected AC 800M controller. 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 the attacker 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?

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, provided that the application and process logic are made in a way that a controller stop leads to a safe shutdown.

What does the update do?

The update removes the vulnerability by modifying the way that the MMS protocol stack verify input data.

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 and all network equipment 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 referenced user manual.

Acknowledgement

ABB thanks the Industrial Control Security Laboratory of Qi An Xin Technology Group Inc. in China for helping to identify the vulnerabilities and protecting our customers.

References

3BSE034463*	System 800xA Reference - Network Configuration
2PAA120527	System 800xA, Symphony Plus and Freelance - System Hardening

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/cyber-security.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2022-02-15