DOCUMENT ID: 3BUA003421
REVISION: B
DATE: 2024-07-18

SECURITY ADVISORY

Multiple Vulnerabilities in ABB Advant MOD 300 AdvaBuild

CVE ID: CVE2020-11639, CVE2020-11640

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 Advant MOD 300 AdvaBuild version 3.0 - 3.7 SP2.

Vulnerability IDs and Product Issue Numbers (PIN)

CVE ID	Product Issue Number*
CVE-2020-11639	ADVABUILD-OL-3702-003
CVE-2020-11640	ADVABUILD-OL-3702-004

* Product Issue Number - is an ABB 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 that the ABB Advant MOD 300 AdvaBuild contains two vulnerabilities which require user attention.

An attacker who successfully exploited these vulnerabilities could elevate his/her privileges to execute arbitrary code, make the system node inaccessible or tamper with runtime data in the system.

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 service accounts.

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 for the computers where AdvaBuild is used.

All the vulnerabilities have been corrected in AdvaBuild version 3.7 SP3 released in April 2021.

ABB recommends that customers apply the update at earliest convenience. Users who are unable to install the update should immediately look to implement the “Mitigating factors” listed below as this will restrict or prevent an attacker’s ability to compromise the system.

Vulnerability severity and details

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

AdvaBuild CVE-2020-11639 – Inter process communication, Insufficient access control

CVSS v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.1 (High)
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C
NVD Summary Link:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11639

AdvaBuild consists of Windows processes. Some of the processes in AdvaBuild 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, effectively 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 disrupts the communication.

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 in 800xA for MOD 300 and AdvaBuild to crash.

AdvaBuild CVE-2020-11640 – Elevation of Privilege

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	7.8 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:C
NVD Summary Link:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11640

AdvaBuild uses a command queue to launch certain operations. An attacker who gains access to the command queue can use it to launch an attack by running any executable on the AdvaBuild node. The executables that can be run are not limited to AdvaBuild specific executables.

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.

1. **CVE-2020-11639 – Inter process communication, Insufficient access control**
   This attack may also be mitigated by application whitelisting. Local access is required to exploit this issue. Please contact ABB for information about how to use application whitelisting on System 800xA.
2. **CVE-2020-11640: – Elevation of Privilege**
   The ability to exploit this issue from a remote connection is mitigated by using the procedure defined in the Product Bulletin 3BUA003423.

Workarounds

No workarounds are available. Assess the installation specific risk based on this advisory. Use the recommendations described under “Recommended immediate actions” and “Mitigating factors”.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could execute arbitrary code or read and write data to/from MOD 300 controllers.

What causes the vulnerability?

CVE-2020-11639: **Inter process communication, Insufficient access control**
The vulnerability is caused by weak access control settings for objects used to exchange information between SW processes on the same computer.

CVE-2020-11640: **Elevation of Privilege**
The vulnerability is caused by a command queue with insufficient protection.

What is AdvaBuild?

AdvaBuild software is the engineering software package for Advant MOD 300 control systems. It supports the project engineering functions of configuration of the Advant OCS control database, plant documentation, development and revision control for TCL sequences and recipes.

What might an attacker use the vulnerability to do?

See “Vulnerability details” above.

How could an attacker exploit the vulnerability?

CVE-2020-11639: **Inter process communication, Insufficient access control**
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.

CVE-2020-11640: **Elevation of Privilege**
An attacker could try to exploit the vulnerability by injecting a command into the affected command queue.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access and access to an account that can login to the computer remotely could exploit these vulnerabilities. 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.

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

Functional safety systems are not affected by these vulnerabilities.

What does the update do?

All the vulnerabilities have been corrected in AdvaBuild version 3.7 SP3 released in April 2021. ABB recommends that end users apply the update at earliest convenience.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, these vulnerabilities were found during internal assessments.

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 these vulnerabilities have 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.

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	2021-12-20
B	all	Update for corrections by AdvaBuild 3.7 SP3.	2024-07-16