DOCUMENT ID: 3BDI100056
REVISION: A
DATE: 2023-11-03

CYBER SECURITY ADVISORY

ActiveMQ vulnerability: impact on ABB Ability™ Genix

CVE ID: CVE-2023-46604

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 de-scribed 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.

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 as 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 Ability™ Genix 21.1, 22.2, 23.1.

Vulnerability IDs

CVE-2023-46604

Summary

ABB is aware of a reported vulnerability in Apache ActiveMQ (CVE-2023-46604) that is used in the ABB Ability™ Genix versions listed in this document.

The steps to upgrade the vulnerable ActiveMQ versions used in ABB Ability™ Genix to existent unaffected ActiveMQ versions will be performed by ABB team working with the customer. This document also describes some mitigations and workaround that can help concerned users limit their risk.

An attacker who successfully exploited this vulnerability could cause the ActiveMQ to stop and could insert and run arbitrary shell commands. In case of ABB Ability™ Genix, it might bring down the ActiveMQ broker and cause other components to be not able to communicate with such broker until it is brought back up.

Recommended immediate actions

ABB has identified steps for the affected Genix versions to upgrade the vulnerable ActiveMQ versions (5.15.9, 5.17.3) to the unaffected versions (5.15.16, 5.17.6) as listed in their official website.

ABB advises affected customers to contact ABB Genix Support to install the mentioned unaffected ActiveMQ versions to address the mentioned vulnerability in ActiveMQ.

Also, it is advised to review the Mitigating factors and Workarounds sections for additional advice on how to reduce the risk associated with this vulnerability.

Vulnerability severity and details

A vulnerability exists in the ActiveMQ third party open-source system included in the product ABB Ability™ Genix versions 21.1, 22,2, 23.1.

In Genix, ActiveMQ is used as a message broker within Genix infrastructure for reliable, asynchronous message delivery from Edge to Cloud.

This vulnerability is a remote code execution vulnerability in Apache ActiveMQ that allows a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the Open Wire protocol to cause the broker to instantiate any class on the class path. The root cause of the issue is insecure deserialization.

The severity assessment has been performed by using the FIRST common Vulnerability Scoring System (CVSS) v3.1 as 10.

CVE 2023-26604 Apache ActiveMQ Deserialization of Untrusted Data Vulnerability

CVSS v3.1 Base Score:	10
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-46604

Impact on ABB Ability™ Genix

The potential impact of the CVE-2023-46604 vulnerability on the Genix architecture is reduced. This is because:

- The exploit is possible using the OpenWire protocol, which is enabled by default on all ActiveMQ deployments. However, the OpenWire protocol is no longer widely used and is disabled in the Genix architecture.
- ActiveMQ is deployed as a separate Azure VMSS container disconnected from the rest of the network or as part of a Kubernetes deployment (on-premise) with ingress rules. This reduces the threat surface and limits the impact of any potential exploit to the container host.
- For ABB-hosted deployments, ActiveMQ is configured to receive data from trusted IP addresses and only allows access to "ABB iboss Proxy" for development and staging environments. This further reduces the risk of exploitation.
- Because Genix uses ActiveMQ in a sandboxed containerized environment the impact if exploited is limited to the container due the ingress and firewall rules in place.

Mitigating factors

The following measures will reduce the vulnerability exploitability:

1. Restrict access to the ActiveMQ broker to only trusted clients. This will reduce the number of potential attackers.
2. Use a web application firewall (WAF). A WAF can be used to block malicious requests that attempt to exploit the vulnerability.

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

Workarounds

Disable the OpenWire protocol. This is the most effective workaround, as it prevents attackers from exploiting the vulnerability. ABB team will work with the customer to apply the changes on immediate basis if they need more time to upgrade. This will only minimize the risk and ABB will strongly recommend to only upgrade to ActiveMQ version which has vulnerability addressed.

Frequently asked questions

What is the scope of the vulnerability?

The scope of CVE-2023-46604 is all versions of Apache ActiveMQ prior to 5.15.16 and 5.17.6. This includes all deployments of ActiveMQ, regardless of the operating system or platform.

The vulnerability can be exploited by a remote, unauthenticated attacker to execute arbitrary code on the ActiveMQ broker.

What causes the vulnerability?

CVE-2023-46604 is caused by an improper validation of serialized class types in the OpenWire protocol. This allows an attacker to send a specially crafted message to the ActiveMQ broker that will cause it to instantiate any class on the class path. The attacker can then use this class to execute arbitrary code on the broker.

What is the affected product or component?

CVE-2023-46604 is in all versions of Genix 21.1, 22.2, 23.1 which includes Apache ActiveMQ prior to 5.15.16 and 5.17.6. This includes all deployments of ActiveMQ, regardless of the operating system or platform.

What might an attacker use the vulnerability to do?

It allows an attacker to execute arbitrary code on the ActiveMQ broker. This could allow the attacker to take control of the broker, steal data, or disrupt operations. In case of Genix, it will bring down the ActiveMQ broker and cause other components to be not able to communicate with the broker until it is brought back up.

How could an attacker exploit the vulnerability?

The attacker can inject any arbitrary code on the ActiveMQ broker. This way, he can take control of the broker, steal data, disrupt operations, bring ActiveMQ broker down and thus can-do malicious things exploiting the vulnerability.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability.

What does the update do?

The update patch will upgrade vulnerable versions of ActiveMQ to the latest versions provided by Apache. The patch updates the ActiveMQ broker to reject untrusted serialized class types. This prevents the attacker from exploiting the vulnerability to instantiate arbitrary classes on the classpath. ABB team will work with the customer to apply the changes on immediate basis.

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

Yes. According to the NVD, the security advisory for CVE-2023-46604 was issued on October 27, 2023, which was the same day that the vulnerability was publicly disclosed. This means that attackers were aware of the vulnerability before the patch was available, which gave them more time to develop and exploit the vulnerability.

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

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any net-work other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- 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.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

ABB Ability™ Genix support : genix-support@abb.com

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	5.Nov.2023

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date