DOCUMENT ID: 9ADB012621
REVISION: D
DATE: 2021-12-17

CYBER SECURITY NOTIFICATION

Apache log4j vulnerabilities (Log4Shell) – impact on ABB products

CVE-2021-44228, CVE-2021-45046, CVE-2021-4104

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 cyber security program which involves not only internal processes to ensure product security but also external engagement with the wider cybersecurity community and 3rd party suppliers. Occasionally an issue is identified with the potential to impact ABB products and systems.

Generally, this means 3rd party product vulnerabilities or life-cycle issues to which ABB products may have a dependency on. Another example could be threats which are not directly targeting ABB products however may constitute a threat to environments where ABB products/systems operate.

When a potential threat is identified or reported, ABB immediately initiates our vulnerability handling process. This entails an evaluation to determine if there are steps which can be taken to reduce risk and maintain functionality for the end user.

The result may be the publication of a Cyber Security Notification. This intends to notify customers of the issue 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 Notification should not be assumed as an 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 Notification is an example of ABB's commitment to the user community in support of this critical topic. The release of a Notification intends to provide timely information which is essential to help ensure our customers are fully informed. See details below and refer to the section on "General security recommendations" for further advise on how to keep your systems secure.

Background

On December 9th, 2021 new vulnerabilities, CVE-2021-44228 (commonly referred to as Log4Shell) and CVE-2021-4104, were made public.

These vulnerabilities may affect a variety of products and solutions which are using the open-source library log4j from the Apache project. Subsequently, a successful exploit could allow attackers to execute arbitrary code on the targeted system without authentication. Exploiting these vulnerabilities requires access to a vulnerable application, which may be over a remote network connection. At the time of writing, there are reports that this vulnerability is exploited in the wild.

With the announcement from the Apache project, it is understood that ABB may need to integrate patches or fixes to address these vulnerabilities in the log4j library for products which are affected, according to the ABB Vulnerability Handling policy. In other scenarios, customers may be able to update the affected library after ABB's validation but without a dedicated update of the ABB product. We are currently analyzing our product portfolio for exposure. Potentially affected customers should expect additional communication or advisories as more details become available.

Potentially affected products

ABB is still investigating the potentially affected products and to date ABB has identified the following products which are likely affected by the vulnerabilities in log4j (ABB products not listed are initially evaluated as not impacted).

© Copyright 2021 ABB. All rights reserved.

Product / System line	Potentially affected products and versions	Status	Link to product specific advisory or notification
B&R Products	See further details in specific advisory		https://www.br-automation.com/downloads_br_productcatalogue/assets/1639507581859-en-original-1.0.pdf
ABB Remote Service	ABB Remote Access Platform (RAP)	Fixed	Details are shared with customers with an active RAP subscription

For more specific guidance e.g., recommended immediate actions, mitigating actions and workarounds, please refer to the product specific notifications and advisories as they become available.

The following products had previously been listed in the table above but have later been concluded as not affected.

Product / System line	Products and versions considered not affected
AlarmInsight Cloud	AlarmInsight KPI Dashboards 1.0.0

Vulnerability Details

See and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104 for more details.

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 network 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.

© Copyright 2021 ABB. All rights reserved.

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	2021-12-15
B	Page 3	Link to B&R notification updated	2021-12-16
C	Page 3	ABB Remote Access Platform (RAP) added	2021-12-16
D	Page ¾	Moved AlarmInsight KPI Dashboards to non-affected Marked ABB Remote Access Platform (RAP) as fixed	2021-12-17

© Copyright 2021 ABB. All rights reserved.