DOCUMENT ID: 2NGA001478
REVISION: A
DATE: 2022-11-21

CYBER SECURITY NOTIFICATION

ARM600 M2M Gateway Aide, Apache, ClamAV, and OpenSSL vulnerabilities

ABBVREP0082

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 following dates, the vulnerabilities below were made public.

- Jan-20-2022, CVE-2021-45417, AIDE
- Jan-14-2022, CVE-2022-20698, ClamAV
- Sep-16-2021, CVE-2021-34798, Apache
- Sep-16-2021, CVE-2021-39275, Apache
- Jun-10-2021, CVE-2021-26691, Apache
- Dec-20-2021, CVE-2021-44790, Apache
- Aug-24-2021, CVE-2021-3712, OpenSSL

These vulnerabilities affect different software components of the ARM600 M2M gateway (see the table below). Subsequently, a successful exploit could allow attackers to cause a denial of service, privilege escalation, or potentially execute code. Exploiting these vulnerabilities varies from low to high complexity.

CSV number	CVSS score	Affected component	Vulnerability	Exploit
CVE-2021-45417	7.8	AIDE	Heap-based buffer overflow	Privilege escalation Complexity: Low

CSV number	CVSS score	Affected component	Vulnerability	Exploit
CVE-2022-20698	7.5	ClamAV	OOXML parsing module	Denial of service Complexity: Low
CVE-2021-34798	7.5	Apache	Null pointer dereference	Denial of service Complexity: Low
CVE-2021-39275	9.8	Apache	Out of bounds write	Denial of service or potentially execute code on httpd user privileges Complexity: Low
CVE-2021-26691	9.8	Apache	Heap overflow	Denial of service Complexity: Low
CVE-2021-44790	9.8	Apache	Buffer overflow	Impact on confidentiality, integrity, and/or availability Complexity: Low
CVE-2021-3712	7.4	OpenSSL	Buffer overrun	Denial of service or potential memory disclosure Complexity: High

Affected products

ABB has identified the following products which are affected by the vulnerability.

Product / System line	Products and Affected Versions
ABB ARM600 M2M Gateway series	ARM600A2500NA, ARM600B2500NA and ARM600C2500NA - up to firmware version 5.0.2
ABB ARM600 M2M Gateway Enterprise Edition series	ARM600A2505NA, ARM600B2505NA and ARM600C2505NA - up to firmware version 5.0.2
ABB ARM600SW M2M Gate-way	ARM600SW1A1, ARM600SW2A3 and ARM600SW3A3 up to firmware version 5.0.2
Older Viola Systems M2M Gateway series	Viola M2M Gateway - all 3.x.x firmware versions
Older Viola Systems M2M Gateway Enterprise Edition series	Viola M2M Gateway Enterprise Edition - all 3.x.x firmware versions

Recommended immediate actions

The problem is corrected in ARM600 firmware version 5.0.3. It can be installed on top of 5.0.1 or 5.0.2 firmware. ABB recommends that customers apply the update at their earliest convenience.

For older ABB ARM600 versions, contact ABB technical support regarding the update path.

No update is planned for older Viola Systems' 3.x.x firmware. Refer to chapter Mitigating factors for reducing the risks with unpatched 3.x.x versions. Alternatively, obtain a new ARM600 server or software product from ABB.

Mitigating factors

Jan-20-2022, CVE-2021-45417, AIDE

- The AIDE can be configured only as a privileged (wheel-group administrator) user. Limit the access of administrator users to internal trusted persons only.
- Go through the list of administrator users and verify the need for user account case-by-case.
- Change the passwords for administrator user accounts.

Jan-14-2022, CVE-2022-20698, ClamAV

- Verify that the ARM600 has no access to the internet for ports and protocols that could be used for transferring a crafted OOXML file to the device (such as SSH, FTP, etc. A crafted OOXML file can be used for exploiting the vulnerability).
- Go through the list of users and verify the need for user account case-by-case.
- Change the passwords for administrator user accounts.

Sep-16-2021, CVE-2021-34798, Apache

- Avoid exposing the Apache web server (WHMI, web human-machine interface) to the internet.
- If external access is needed, an OpenVPN client can be used.

Sep-16-2021, CVE-2021-39275, Apache

- Avoid exposing the Apache web server (WHMI) to the internet.
- If an external access is needed, an OpenVPN client can be used.

Jun-10-2021, CVE-2021-26691, Apache

- Avoid exposing the Apache web server (WHMI) to the internet.
- If an external access is needed, an OpenVPN client can be used.

Dec-20-2021, CVE-2021-44790, Apache

- Avoid exposing the Apache web server (WHMI) to the internet.
- If an external access is needed, an OpenVPN client can be used.

Aug-24-2021, CVE-2021-3712, OpenSSL

- Avoid exposing WHMI interface to the internet.
- If external access is needed, an OpenVPN client can be used.

Vulnerability Details

See the following links for more details.

- Jan-20-2022, CVE-2021-45417, AIDE: https://nvd.nist.gov/vuln/detail/CVE-2021-45417
- Jan-14-2022, CVE-2022-20698, ClamAV: https://nvd.nist.gov/vuln/detail/CVE-2022-20698
- Sep-16-2021, CVE-2021-34798, Apache: https://nvd.nist.gov/vuln/detail/CVE-2021-34798
- Sep-16-2021, CVE-2021-39275, Apache: https://nvd.nist.gov/vuln/detail/CVE-2021-39275
- Jun-10-2021, CVE-2021-26691, Apache: https://nvd.nist.gov/vuln/detail/CVE-2021-26691
- Dec-20-2021, CVE-2021-44790, Apache: https://nvd.nist.gov/vuln/detail/CVE-2021-44790
- Aug-24-2021, CVE-2021-3712, OpenSSL: https://nvd.nist.gov/vuln/detail/cve-2021-3712

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 programming 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 connected devices.

More information on recommended practices can be found in the following document:

1MRS758860 revision F: Arctic, Cyber Security Deployment Guideline

Support

For additional instructions and support, please get in touch with 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	Nov-21-2022