DOCUMENT ID: 2NGA001478
REVISION: B
DATE: 2023-03-07

CYBER SECURITY ADVISORY

ABB ARM600 M2M Gateway Aide, Apache, Clam AV, and OpenSSL vulnerabilities

CVE ID: CVE-2021-45417, CVE-2022-20698, CVE-2021-34798, CVE-2021-39275, CVE-2021-26691, CVE-2021-44790, CVE-2021-3712

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 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 has identified the following products that are affected by vulnerabilities.

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 Gateway	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

Vulnerability IDs

CVE-2021-45417, CVE-2022-20698, CVE-2021-34798, CVE-2021-39275, CVE-2021-26691, CVE-2021-44790, CVE-2021-3712

ABBVREP0082

Summary

Updates are available that resolve publicly reported vulnerabilities in the product versions listed above.

An attacker who successfully exploits these vulnerabilities could make the product inaccessible, elevate user privileges or insert and run arbitrary code.

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.

For older Viola Systems' 3.x.x firmware refer to the chapter "Mitigating factors" for reducing risks. Alternatively, obtain a new ARM600 server or software product from ABB.

Vulnerability severity and details

Vulnerabilities exist in the multiple components included in the product versions listed above. An attacker could exploit these vulnerabilities by sending a specially crafted message to the system node causing the node to stop, or become inaccessible, allowing the attacker to elevate user privileges, take control of the product, or allow the attacker to insert and run arbitrary code.

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

CSV number	CVSS score	Affected component	Vulnerability	Exploit
				Complexity: Low
CVE-2021-3712	7.4	OpenSSL	Buffer overrun	Denial of service or potential memory disclosure Complexity: High

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

CVE-2021-45417, Aide

AIDE before 0.17.4 allows local users to obtain root privileges via crafted file metadata (such as XFS extended attributes or tmpfs ACLs), because of a heap-based buffer overflow.

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.2
CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-45417

CVE-2022-20698, ClamAV

A vulnerability in the OOXML parsing module in Clam AntiVirus (ClamAV) Software version 0.104.1 and LTS version 0.103.4 and prior versions could allow an unauthenticated, remote attacker to cause a denial-of-service condition on an affected device. The vulnerability is due to improper checks that may result in an invalid pointer read. An attacker could exploit this vulnerability by sending a crafted OOXML file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial-of-service condition.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 6.7
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-20698

CVE-2021-34798, Apache

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS v3.1 Base Score: 7.5

[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.

CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/cve-2021-34798

CVE-2021-39275, Apache

The ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party/external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.8
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/cve-2021-39275

CVE-2021-26691, Apache

In Apache HTTP Server versions 2.4.0 to 2.4.46, a specially crafted SessionHeader sent by an origin server could cause a heap overflow.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.8
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-26691

CVE-2021-44790, Apache

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.5
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-44790

CVE-2021-3712, OpenSSL

ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function, will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array.

If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions, then this issue could be hit. This might result in a crash (causing a Denial-of-Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

CVSS v3.1 Base Score:	7.4
CVSS v3.1 Temporal Score:	6.7
CVSS v3.1 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/cve-2021-3712

Mitigating factors

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.

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 files to the device (such as SSH, FTP, etc.). A crafted OOXML file can be used to exploit 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.

CVE-2021-34798, CVE-2021-39275, CVE-2021-26691, CVE-2021-44790, 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.

CVE-2021-3712, OpenSSL

- Avoid exposing the WHMI (web human-machine interface) to the internet.
- Consider using a cellular private access point for VPN traffic.

In addition to the mitigating factors, refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

What is the scope of these vulnerabilities?

An attacker who successfully exploited these vulnerabilities could prevent legitimate access to an affected system node or remotely cause an affected system node to stop (CVE-2022-20698, CVE-2021-34798, CVE-2021-34798, CVE-2021-39275, CVE-2021-26691, CVE-2021-44790, CVE-2021-3712), take control of an affected system node (CVE-2021-39275, CVE-2021-44790), insert and run arbitrary code in an affected system node (CVE-2021-39275, CVE-2021-44790) or elevate user privileges from non-privileged user to privileged user (CVE-2021-45417).

What causes the vulnerabilities?

The vulnerabilities are caused by the following:

- CVE-2021-45417, Aide: In the base64 encoding functionality of Aide, there is a dynamically allocated memory buffer overflow vulnerability can be exploited.
- CVE-2022-20698, ClamAV: In the OOXML (Open Office XML) parser, there are improper checks for the validity of the OOXML that may result in an invalid pointer being read.
- CVE-2021-34798, Apache: Malformed requests may cause the server to point to a non-existing memory location or non-real memory address. When data is read/written to an improper address, it may cause undefined behavior.
- CVE-2021-39275, Apache: A function may write beyond the end of a buffer when given malicious input via e.g., a third-party Apache module.
- CVE-2021-26691, Apache: In the mod_auth_digest module of Apace, there is a vulnerability that can be exploited by crafted session headers.
- CVE-2021-44790, Apache: In the mod_lua parser module of Apache, there is a buffer overflow vulnerability that can allow out-of-bounds data writing by a crafted request.
- CVE-2021-3712, OpenSSL: The ASN.1 (Abstract Syntax Notation One) strings are parsed by OpenSSL using internal functions. If an application constructs an ASN.1 string that is not NUL terminated, a read buffer overrun can happen.

What are these software components?

The following ARM600 software components are affected:

- Aide (Advanced Intrusion Detection Environment) is a software that takes a snapshot of the computer's configuration, and the original snapshot data is compared to the later changes of the configuration, thus revealing any changes that may have been done by an attacker.
- ClamAV (Clam AntiVirus) is an antimalware toolkit that detects many types of malware, including viruses.
- Apache is a web server providing a WHMI in ARM600.
- OpenSSL is a cryptography library that offers an application of the TLS protocol.

What might an attacker use these vulnerabilities to do?

An attacker who successfully exploits these vulnerabilities could cause the affected system node to stop or become inaccessible or to be taken into control by the attacker to allow elevating user's privileges or to allow the attacker to insert and run arbitrary code in the system.

How could an attacker exploit these vulnerabilities?

An attacker could try to exploit the vulnerabilities by creating a specially crafted message and sending the message to an affected system node. 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 he 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 these vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node 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.

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

Depending on the use case, the attacker could, e.g., stop legitimate users from remotely operating switching objects by exploiting these vulnerabilities.

What does the update do?

The update completely removes these vulnerabilities by modifying the way that the components are e.g., validating messages or verifying the input data.

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

Yes, these vulnerabilities have been publicly disclosed.

When this security advisory was issued, had ABB received any reports that these vulnerabilities were being exploited?

No, ABB had not received any information indicating that these vulnerabilities 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 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.

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 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	Nov-21-2022
B	5,6	Revision B, changed the title to "Advisory", and added FAQ	March-07-2022