DOCUMENT ID: 2NGA001254
REVISION: A
DATE: 2022-04-11

CYBER SECURITY NOTIFICATION

ARM600 M2M Gateway
NSS library and polkit vulnerabilities

ABBVREP0071

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.

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 "General security recommendations" for further advise on how to keep your systems secure.

Background

On Dec-08-2021 and on Jan-25-2022 two vulnerabilities, NSS library (CVE-2021-43527) and Polkit (CVE-2021-4034) were made public.

These vulnerabilities affect cryptographic libraries and privilege handling. Subsequently, a successful exploit could allow attackers to execute code with root user privileges or to elevate a non-privileged user to a privileged user. Exploiting the NSS vulnerability requires complex attack methods in the ARM600 environment, whereas exploiting the Polkit vulnerability would be less complex for the authenticated nonprivileged user.

Related products

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

NSS library vulnerability

The products listed in the table are affected by the vulnerability.

Product / System line	Products and Affected Versions	Notification
ABB ARM600 M2M Gateway series	ARM600A2500NA, ARM600B2500NA, and ARM600C2500NA - up to firmware version 5.0.1	Notification
ABB ARM600 M2M Gateway Enterprise Edition series	ARM600A2505NA, ARM600B2505NA, and ARM600C2505NA - up to firmware version 5.0.1	
ABB ARM600SW M2M Gateway	ARM600SW1A1, ARM600SW2A3, and ARM600SW3A3 up to firmware version 5.0.1	
Older Viola Systems M2M Gateway series	Viola M2M Gateway - all 3.x.x firmware versions	Notification
Older Viola Systems M2M Gateway Enterprise Edition series	Viola M2M Gateway Enterprise Edition - all 3.x.x firmware versions	

Polkit vulnerability

The products listed in the table are affected by the vulnerability.

Product / System line	Products and Affected Versions	Notification
ABB ARM600 M2M Gateway series	ARM600A2500NA, ARM600B2500NA, and ARM600C2500NA - up to firmware version 5.0.2	Notification
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	Notification
Older Viola Systems M2M Gateway Enterprise Edition series	Viola M2M Gateway Enterprise Edition - all 3.x.x firmware versions	

Recommended immediate actions

NSS library vulnerability

ABB ARM600

ABB recommends that customers would apply the update to the ARM600 M2M Gateway firmware 5.0.2 at earliest convenience.

How to update:

1. Any older ABB ARM600 firmware version can be updated to the 5.0.1 version with “updateinstaller” script. The script and instructions can be obtained from ABB technical support.
2. Once the firmware is in 5.0.1 level, the system can be updated to firmware 5.0.2 with “systemupdate” command. Please refer to ARM600 User Manual, document ID 1MRS758861, revision G, chapter 9.1 (for hardware variants) or chapter 9.2 (for software variants).

Viola Systems M2M Gateway

At the moment, there are no further firmware updates planned for these devices. There is no mitigation available in operating system level. See the "Mitigating factors" and "General security recommendations" chapters for other mitigation actions.

Polkit vulnerability

There are no recommended immediate actions regarding patching. See the "Mitigating factors" and "General security recommendations" chapters for mitigation actions.

Mitigating factors

NSS library vulnerability

ABB ARM600

- Update to 5.0.2 firmware, which completely resolves the issue by fixing the flaw in the NSS library.
- If the immediate firmware update is not possible, consider using a local DNS. The curl software that is used in ARM600 has a dependency to NSS software. The curl software is used for checking new firmware updates from https://arcticupdate.abb.com/ server and for opening the Arctic wireless gateway's web HMI via ARM600 Patrol management application's "Devices" page. Using a local DNS prevents from DNS spoofing attacks that could be combined with NSS vulnerability exploit.

Viola Systems M2M Gateway

- Consider using a local DNS. Since the curl software that is used in Viola M2M Gateway has a dependency to NSS software it is recommended to use a local DNS. The curl software is used for opening the Arctic wireless gateway's web HMI via ARM600 Patrol management application's

"Devices" page. Using a local DNS prevents from DNS spoofing attacks that could be combined with NSS vulnerability exploit.

- It is recommended to use a private cellular access point for mobile device connections.
- Alternatively, it is recommended to replace the device with a new ABB ARM600 M2M Gateway.

Polkit vulnerability

ABB ARM600

- Identify the non-privileged users that can access the system, and possibly limit the number of users to trusted internal users.
- Use personal user accounts rather than shared accounts.
- Change passwords for preventing the use of previously shared passwords.

Viola Systems M2M Gateway

- Identify the non-privileged users that can access the system and possibly limit the number of users to trusted internal users.
- Change passwords for preventing the use of previously shared passwords.

Additional information

NSS library vulnerability

The NSS consists of crypto libraries, utilities, and APIs for security-enabled client and server applications. The NSS library is included in the operating system of ABB ARM600 and Viola Systems M2M Gateway. The versions of NSS prior to 3.73 or 3.68.1 ESR are vulnerable.

There is a data bounds-check vulnerability in handling the digital key signature data. Fixed 2048 bytes is reserved in the digital signature verification structure of NSS, (i.e., 16384 bits of RSA maximum modulus). If a crafted untrusted signature exceeds the fixed limit, heap overflow and thus memory corruption happens. This may allow the attacker to execute arbitrary code.

Polkit vulnerability

The polkit is included in the operating system of ABB ARM600 and Viola Systems M2M Gateway. There is a flaw in pkexec program that is causing the vulnerability. The versions of polkit prior to polkit-0.112-26.el7_9.1.x86_64 are vulnerable.

The polkit's pkexec program is by default installed in many Linux systems and it is used for controlling operation system-wide privileges, allowing an authorized user to execute specific programs as another user. The vulnerability in pkexec allows an unprivileged (but authorized) user to gain full root privileges on a vulnerable host by exploiting this vulnerability.

By manipulating the path variable and command-line arguments the attacker can cause an out-of-bounds write to pkexec's main function, which in turn allows the attacker to enter an insecure environment variable to pkexec's environment. When manipulating the argument and environment arrays, the attacker can execute payloads as a privileged user without authentication.

Vulnerability Details

See the following links for more details.
NSS vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2021-43527
Polkit vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2021-4034

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	April-11-2022