ABB DOC ID: 2NGA000784
REVISION: -
DATE: 2020-12-02

CYBER SECURITY ADVISORY

Arctic wireless gateway Firewall Configuration

ABBVU-VREP0030-ELDS2048-24684

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.

Affected Products

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

Product / System line	Products and Affected Versions	Advisory
ABB Arctic wireless gateway series	ARG600/ARC600/ARP600/ARR600 Category - up to firmware version 3.4.9	Advisory
Older ABB and Viola Systems Arctic wireless gateway series	Viola Systems' Arctic gateway versions with HTTPS user interface support	Advisory
	ABB REC/RER 601/603, Viola Systems' Arctic wireless gateway versions with HTTP user interface support and Viola Systems' Arctic 3G gateway 2620	Advisory

ABB products not listed are initially evaluated as not impacted. ABB continues to evaluate the vulnerabilities and will update the advisory when additional information becomes available

Vulnerability ID

ABB ID: ABBVU-VREP0030-ELDS2048-24684
CVE ID: CVE-2020-24684

Summary

The Arctic wireless gateways are configured as WAN gateway by default.

- ABB Arctic wireless gateways have the firewall enabled by default, allowing outgoing traffic from LAN to the Internet but blocking all incoming traffic. When activating VPN it is possible that Ethernet-connected devices in Arctic wireless gateway's LAN can access the internet, even though the VPN routing setting of the "Default route".
- The older Viola Systems Arctic wireless gateways are also affected, and the mitigation depends on gateway version.

This is not clearly mentioned in the web UI or in the product documentation. It has been found that this is not clearly understood by customers.

ABB has published an updated cybersecurity deployment guideline for the Arctic wireless gateways "1MRS758860", the document is available at ABB library https://library.abb.com/.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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 Base Score: 4.7

CVSS v3 Temporal Score: 4.2

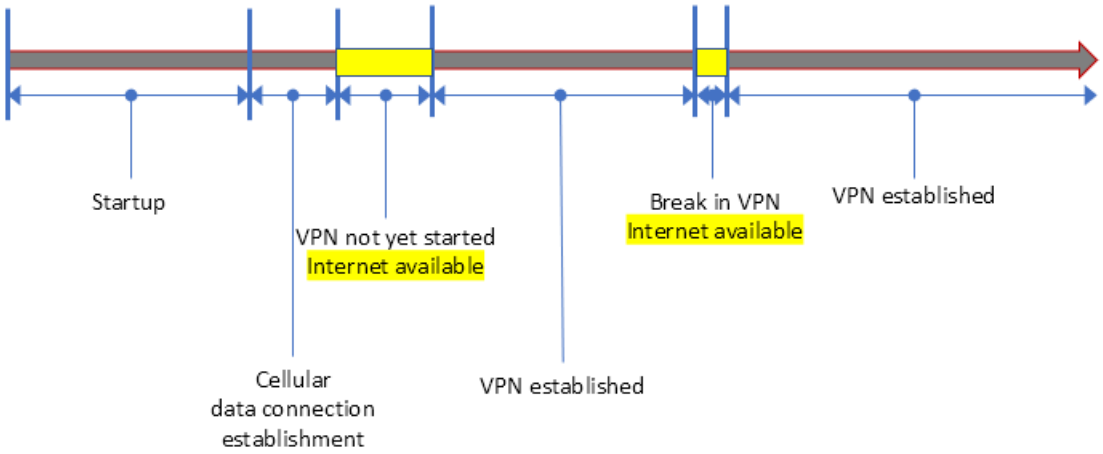
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N/E:U/RL:T/RC:C

CVSS v3 Link:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N/E:U/RL:T/RC:C/

Vulnerability Details

With certain configurations of ABB Arctic wireless gateway, it is possible that Ethernet-connected devices in Arctic wireless gateway's LAN can access the internet, even though the VPN routing setting is "Default route". It happens when the VPN tunnel is not established; in the device's boot up phase, in VPN reconnection phase or when the VPN tunnel fails to be established.



Mitigating Factors

This cybersecurity advisory describes how to configure the gateway to avoid fallback to WAN functionality. Then outbound internet access is disabled during boot and when VPN breaks.

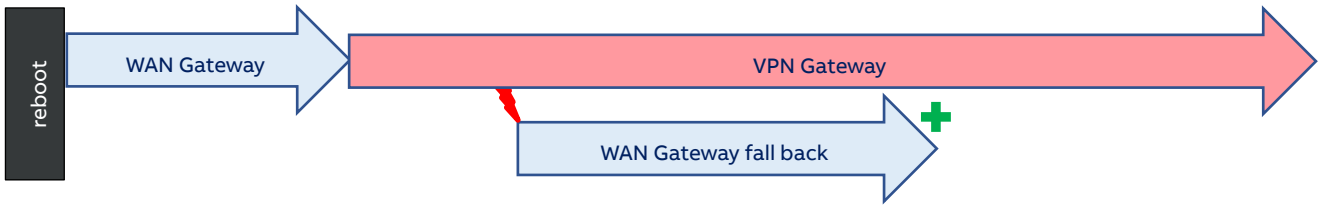
Advisory for ABB Arctic wireless gateways

These are the different configurations and the steps to configure them in an Arctic gateway:

Default Configuration – WAN Gateway

In the default configuration the gateway acts as a WAN gateway. It allows outgoing traffic from LAN to the Internet by default and blocks all incoming traffic.

VPN Gateway with WAN Gateway fallback



In this configuration the gateway will switch to a VPN tunnel. However, during startup and when the VPN tunnel fails it will act as a WAN gateway.

How to configure:

1. Create or import the VPN configuration
2. In VPN routing settings, set the VPN tunnel as "default GW" or enter the subnet/netmask for the network, which is reachable via VPN tunnel. If using OpenVPN with "push routes", it is not necessary to define any routing in the client side.

For configuration details please refer to the manuals:

- For ARM600 M2M GW, see chapter 5.4 in User Manual, 1MRS758861, revision C.
- For Arctic wireless GW, see chapter 5.3 in User Manual, 1MRS758456, revision D.

VPN Gateway only

In this configuration the gateway will act as a pure VPN gateway. If the VPN connection fails, there will be no connection at all.

How to configure:

1. Create or import the VPN configuration
2. In VPN routing settings, set the VPN tunnel as "default route" or define the subnet/netmask of a network, which is reachable via VPN tunnel. If using OpenVPN with "push routes", it is not necessary to define any routing in the client side.
   Ensure that the firewall's default actions for incoming and forwarded traffic are "Drop" in Firewall --> General page.
3. In Firewall --> General page, set the "LAN-Out accepted" as "No".

For configuration details please refer to the manuals:

- For ARM600 M2M GW, see chapter 5.4 in User Manual, 1MRS758861, revision C.
- For Arctic wireless GW, see chapter 5.3 in User Manual, 1MRS758456, revision D.

Advisory for ABB REC/RER 601/603, Viola Systems Arctic wireless gateways with HTTP user interface and Viola Systems 3G gateway 2620

At the moment there are no further firmware updates planned for these gateways. It is recommended to ensure that these gateways are connected to the internet via an external firewall or to use a private APN.

Alternatively, it is recommended to replace them with a newer Arctic Gateway.

Advisory for Viola Systems Arctic wireless gateways with HTTPS user interface

ABB recommends that customers apply the update to the newest Arctic gateway firmware at earliest convenience. Then the configuration advisories for the Arctic Gateways can be applied.

Frequently Asked Questions

What is the scope of the vulnerability?

A system connected to the LAN of the Arctic GW can access the internet during gateway startup and when VPN connection breaks. Thus, a device connected to the LAN could access the internet directly, without VPN default route enforced.

This is not necessarily an unintended behavior, but the user should be aware of that.

What causes the vulnerability?

The description in the UI and manuals did not clearly outline that additional step must be taken to suppress internet connectivity in case VPN connection fails.

Does the advisory mitigate the issue?

Yes, the measures shown in the advisory mitigate the issue completely. There are no further actions needed.

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

Yes, ABB also published the vulnerability via Finnish National Cybersecurity Center.

Support

For additional information and support please contact your product provider or ABB service organization. For contact information, see https://new.abb.com/contact-centers Information about ABB's cyber security program and capabilities can be found at https://www.abb.com/cybersecurity.