PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #01/2020

Automation Runtime SNMP Authentication and Authorization Weakness

Document Version: 1.0

First published: 2020-02-19
Last updated: N/A (Initial version)

Executive Summary

An authentication weakness in the SNMP service in B&R Automation Runtime versions 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, 4.72 and above allows unauthenticated users to modify the configuration of B&R products via SNMP.

Affected Products

Affected products: Automation Studio (AS) and Automation Runtime (AR)
Affected versions: All versions listed in Table 1 are affected

Affected AS version	Associated AR version[1]
2.7	2.96
3.0.71	2.96
3.0.80	3.00, 3.01
3.0.81	3.06, 3.07
3.0.90	3.08 to 3.10, 4.00 to 4.03
4.0.x to 4.6.4	4.04 to 4.63
4.7.2	4.72

Table 1: Affected versions

The following AS versions are **not affected:**

- AS 4.6.5 and higher
- AS 4.7.3 and higher
- AS 4.8.1 and higher

Details about B&R software versioning schemes are outlined in AS help page with GUID 51b2a741-a05d-48c1-957c-2aa1ad5cc8d4.[2]

Vulnerability ID

CVE-2019-19108 Automation Runtime SNMP Authentication and Authorization Weakness

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2019-19108 Automation Runtime SNMP Authentication and Authorization Weakness

CVSS v3 Base Score: 9.4 (Critical)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

[1] Table 1 lists only those AR versions that feature the SNMP service. Old AR versions lacking the SNMP service feature are not listed.
[2] Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 7.

Corrective Actions or Resolution

Due to product-technical reasons, the SNMP credentials cannot be changed.
To reduce risks arising from this vulnerability, the following AS versions disable the SNMP service by default in newly created AS projects:

- AS 4.6.5 (Planned release date: 2020-03-27) and higher
- AS 4.7.3 (Planned release date: 2020-04-10) and higher
- AS 4.8.2 (Planned release date: 2020-06-11) and higher

The above mentioned dates denoted as planned are preliminary and may be subject to change.
Registered customers may approach their local B&R service organization in case of questions.

B&R recommends to take the following measures at the earliest convenience.
Depending on whether you are working on an existing AS project or starting a new AS project, whether you are working with an AS version that is affected by this vulnerability or are already working with an AS version that is no longer affected, different recommendations apply in the respective situation, as shown in Table 2.

	Existing AS project	**New AS project**
Affected AS version	Mitigate SNMP Risks	Mitigate SNMP Risks
Non-affected AS version	Mitigate SNMP Risks	Leave SNMP Disabled

Table 2: Overview of recommendations depending on the initial situation

Mitigate SNMP Risks

Check if you require the SNMP service on your AR devices – this service is typically used for browsing for AR devices (target systems) in AS.
In case you are unsure if you require the SNMP service, please consult your system integrator or your local B&R service organization.

Please note:
The SNMP service is available at Ethernet interface[3] level - each Ethernet interface has its own SNMP configuration. To disable the SNMP service for a whole control system, SNMP has to be disabled on each individual Ethernet interface.

- In case you do **not** require the SNMP service on your AR devices, perform the following steps on every AR device:
  - Open the project used on your AR device in AS
  - Disable the SNMP service in the configuration of **all** Ethernet interfaces
  - Transfer the project to the AR device

  Information on configuring the SNMP service is presented in AS help pages with the following GUID:
  - 376a03a6-7122-418a-9dd3-421aad48abfb (SNMP service configuration – see section "SNMP parameters")
  - 0c62bbc4-d9ec-4cfd-90f9-02b932719d8c (Configuration of Ethernet connection to AR device)

  Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 7.

- In case you need the SNMP service on your AR devices, please take the following protective measures:

[3] The term "Ethernet interface" refers to all Ethernet-capable network interfaces. Examples of such interfaces include standard Ethernet interfaces (e.g. "IF2" on an X20 PLC) and POWERLINK interfaces set to Ethernet operating mode.

    - Restrict SNMP access to AR devices as much as possible e.g. on firewalls or IPS systems
        - Limit SNMP access to relevant source devices and block all other sources
        - If you do not use write access (SNMP SET commands), block any SNMP write access targeting AR devices
    - Take additional safeguarding measures as outlined in section "General Security Guidelines for Control Systems and Control Network" on page 5

- Upgrade AS to a version which disables the SNMP service by default (see above)
    - Newly created projects will automatically disable the SNMP service – this service would need to be enabled manually
    - Existing projects need manual intervention – very likely, they have the SNMP service enabled and it has to be disabled

Leave SNMP Disabled

When creating a new project in a non-affected AS version, the SNMP service is disabled by default. Provided that you do not need the SNMP service, please leave the SNMP service disabled to protect your AR devices from this vulnerability.
In case you do need the SNMP service, please take protective measures as outlined in section "Mitigate SNMP Risks" above.

Vulnerability Details

CVE-2019-19108 Automation Runtime SNMP Authentication and Authorization Weakness

Description
Vulnerable software component: AR SNMP service

AR features an SNMP service supporting read and write access to the device configuration.
The SNMP service has the following security-relevant limitations:

- The name of the SNMP user account is hardcoded and cannot be changed by the user
- The SNMP user account has no password assigned
- SNMP data is transmitted in plain text over the network

Impact
If certain prerequisites are met, an attacker can leverage this vulnerability to perform unauthorized configuration changes on affected devices, resulting in the following potential impacts:

- Network communication problems (e.g. affected device loses connection to systems located in other network segments)
- Loss of network connection (communication between affected device and all other systems stops working)
- Denial of service due to loss of network connection

Fix
Due to product-technical reasons, the SNMP credentials cannot be changed and B&R is not able to provide a patch for this vulnerability.
In order to minimize risks arising from this vulnerability, please refer to section "Corrective Actions or Resolution" above.

Mitigating Factors

Recommended security practices can help to protect control systems and control networks from attacks. Such security practices are outlined in section "General Security Guidelines for Control Systems and Control Network".

Workarounds

In case it is not feasible for you to disable the SNMP service on your AR devices, a workaround is to restrict access to those devices as outlined in section "Corrective Actions or Resolution" above.

General Security Guidelines for Control Systems and Control Networks

Exploits leveraging the vulnerabilities mentioned above and many other threats put control systems[4] and the control network[5] at risk. Customers are strongly advised to take the following safeguarding measures to minimize such risks:

- Place control systems in a dedicated control network containing control systems only.
- Locate control networks and systems behind firewalls and isolate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.
- If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic").
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.
- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please note that VPN solutions may have vulnerabilities and should be updated to the most current version available.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- Limit privileges of user accounts, software processes and devices to those privileges required for normal control operation.

[4] The term "control systems" refers to all kinds of B&R products like PLCs (e.g. X20), visualization systems (e.g. Power Panel T30), process control systems (e.g. APROL) and supporting systems like engineering workstations running Automation Studio.

[5] The term "control network" refers to computer networks used to interconnect control systems. The control network can be subdivided into zones and there can be multiple separate control networks within one company or site.

- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.
- For further support on control system security measures please contact your IT service provider and follow industry accepted security best practices.

Important note:
Please use caution when implementing safeguarding measures and thoroughly test them in advance. It is your responsibility to ensure that such measures do not have side effects that would interfere with normal control operation at your site.

Frequently Asked Questions

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

No, B&R received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had B&R received any reports that this vulnerability was being exploited?

No, B&R had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

B&R would like to thank the following for working with us to help protect our customers:
- Yehuda Anikster and Amir Preminger of Claroty

References

Support

For additional information and support, please contact your local B&R service organization. For contact information, see www.br-automation.com.

Document History

Version	Date	Description
1.0	2020-02-19	Initial version

Appendix

Accessing a help page via GUID

To go to a help page using a GUID, do the following in the AS Help Explorer:

- Press Ctrl + G or select View > Goto Page
- Enter the GUID of the help page as shown in the following screenshot: