Security Advisory
Privilege Escalation via sudo and Linux kernel

1 Advisory Information

Advisory ID: BOSCH-SA-372917

CVE Numbers and CVSS v3.1 Scores:

- CVE-2020-29661
  - Base Score: 7.8 (High)
- CVE-2021-3156
  - Base Score: 7.8 (High)
- CVE-2021-3347
  - Base Score: 7.8 (High)

Published: 24 Feb 2021

Last Updated: 24 Feb 2021

2 Summary

Linux kernel versions through 5.10.11 contain weaknesses, which allow local users to execute code in the kernel with the potential to escalate privileges [1][2] In versions of sudo before 1.9.5p2 there is a weakness present, which allows privilege escalation to root for local users. [3]

The ctrlX CORE and the IoT Gateway both are shipped with vulnerable versions of those components.

To exploit the vulnerabilities, access via terminal or Secure shell (SSH) is required.

3 Affected Products

- ctrlX CORE Runtime < XCR-V0108
- IoT Gateway on IndraControl PR21: PR2100.1-*-IOTNN variants

4 Solution and Mitigations

4.1 Software Update

The next release of ctrlX CORE V0108 includes updated versions of both, kernel and sudo. Please contact your sales partner for instructions on how to retrieve the updates. If your device is connected to the update servers or you manage the devices remotely, the updates can also be applied via the online channel. It is recommended that the updates are installed in a timely manner after their release, if possible.

For IoT Gateway, no updates are available. Please see the following chapters and the IoT Gateway Security Guidelines [5] for compensatory measures

4.2 Compensatory Measures

4.2.1 ctrlX CORE

To exploit one of the vulnerabilities, a user account on the system and access via serial console or secure shell (SSH) is required. Access to the serial console requires opening the housing. SSH is considered a debug interface and therefore is disabled by default on the ctrlX CORE. Additionally, only accounts with a membership in the “sshuser” group are permitted to access the system via SSH. By default, newly created user accounts are not a member of this group. SSH is not required for regular operation of the device.
It is therefore strongly recommended to leave SSH disabled and only enable SSH only temporary when required. Only select users should be granted SSH access via the “sshuser” group.

4.2.2 IoT Gateway

On the IoT Gateway, the single user account on the system already has superuser privileges. By default, no other accounts exist. Therefore, as recommended in the manual [5], the default password shall be changed and kept secret. Compensatory measures are required to mitigate the risk. Always define such compensatory measures individually, in the context of the operational environment. Some possible measures are described in the “Security Guideline Electric Drives and Controls”, for example the network segmentation (please see [4]). In general, it is highly recommended to implement the measures described in the “Security Guideline Electric Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2020-29661

This vulnerability affects ctrlX CORE and the Rexroth IoT Gateway on IndraControl PR21: PR2100.1-*-IOTNN variants.

CVE description: A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.

- Problem Type:
  - CWE-416
  - CWE-667
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

5.2 CVE-2021-3156

This vulnerability affects ctrlX CORE and the Rexroth IoT Gateway on IndraControl PR21: PR2100.1-*-IOTNN variants.

CVE description: Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation to root via “sudoedit -s” and a command-line argument that ends with a single backslash character.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

5.3 CVE-2021-3347

This vulnerability affects ctrlX CORE and the Rexroth IoT Gateway on IndraControl PR21: PR2100.1-*-IOTNN variants.

CVE description: An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.

- Problem Type:
  - CWE-416
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

6 Additional Resources

[1] MITRE CVE-2020-29661: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29661
[2] MITRE CVE 2021-3347: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3347
[3] MITRE CVE 2021-3156: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156
[4] Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562
[5] Bosch Rexroth IoT Gateway Security Guidelines
https://www.boschrexroth.com/documents/12605/22475107/Security+Manual+%E2%80%93+IoT+Gateway+Software+V3/7c805247-efed-915e-5381-28fc4179e445?version=1.1&download=true

7 Revision History

24 Feb 2021: Initial Publication