Security Advisory
Multiple vulnerabilities in ctrlX CORE and IoT Gateway

1 Advisory Information

Advisory ID: BOSCH-SA-918106
CVE Numbers and CVSS v3.1 Scores:

- CVE-2020-27815
  - Base Score: 7.4 (High)
- CVE-2020-27830
  - Base Score: 5.5 (Medium)
- CVE-2020-28374
  - Base Score: 8.1 (High)
- CVE-2020-28941
  - Base Score: 5.5 (Medium)
- CVE-2020-29568
  - Base Score: 6.5 (Medium)
- CVE-2020-29569
  - Base Score: 8.8 (High)
- CVE-2020-29660
  - Base Score: 4.4 (Medium)
- CVE-2020-29661
  - Base Score: 7.8 (High)
- CVE-2021-20232
  - Base Score: 7.4 (High)
- CVE-2021-24031
  - Base Score: 9.1 (Critical)
- CVE-2021-24032
  - Base Score: 9.1 (Critical)
- CVE-2021-27218
  - Base Score: 7.5 (High)
- CVE-2021-27219
  - Base Score: 7.5 (High)
- CVE-2021-27803
  - Base Score: 7.5 (High)

Published: 23 Apr 2021
Last Updated: 23 Apr 2021

2 Summary

Multiple vulnerabilities in operating system libraries and the Linux kernel have been reported which in a worst case scenario could allow an attacker to compromise the system by provoking a crash or the execution of malicious code. The affected functions are not used directly by any Rexroth software component and therefore the risk of an attacker being able to exploit the vulnerability is considered as low. Nevertheless, it cannot be

completely ruled out that the functions might be called indirectly. It is therefore strongly advised to follow the suggested solution and mitigations.

The following CVEs, which are not yet available in the NVD also affect the ctrlX CORE Runtime: CVE-2020-27815, CVE-2020-27830

3 Affected Products

- ctrlX CORE Runtime < XCR-V-0108.1 (Linux kernel)
  - CVE-2020-27815
  - CVE-2020-27830
  - CVE-2020-28374
  - CVE-2020-28941
  - CVE-2020-29568
  - CVE-2020-29569
  - CVE-2020-29660
  - CVE-2020-29661
- ctrlX CORE Runtime <= XCR-V-0108.1 (operating system libraries)
  - CVE-2021-20232
  - CVE-2021-24031
  - CVE-2021-24032
  - CVE-2021-27218
  - CVE-2021-27219
  - CVE-2021-27803
- IoT Gateway (all versions)
  - CVE-2020-27815
  - CVE-2020-27830
  - CVE-2020-28374
  - CVE-2020-28941
  - CVE-2020-29568
  - CVE-2020-29569
  - CVE-2020-29660
  - CVE-2020-29661
  - CVE-2021-20232
  - CVE-2021-24031
  - CVE-2021-24032
  - CVE-2021-27218
  - CVE-2021-27219
  - CVE-2021-27803

4 Solution and Mitigations

4.1 Software Update

For the ctrlX CORE, the Linux kernel vulnerabilities are addressed with XCR-V-0108. Please update your installation to this release if not already done. For the ctrlX CORE operating system libraries vulnerabilities, an updated release is scheduled for 05/2021. 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.

4.2 Compensatory Measures

Compensatory measures are recommended which mitigate the risk are recommended until the update becomes available. 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 [1]). 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-2020-27815

It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service (system crash).

Ubuntu has issued an update for kernel that fixes this and multiple vulnerabilities.

CVE description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.4 (High)

5.2 CVE-2020-27830

Vulnerability found in Linux Kernel, which can lead to a crash.

CVE description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 5.5 (Medium)

5.3 CVE-2020-28374

Vulnerability in the Linux Kernel that could allow attackers to read or write files.

CVE description: In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.

- Problem Type:
  - CWE-22
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
  - Base Score: 8.1 (High)

5.4 CVE-2020-28941

An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers could cause a local denial of service attack.

CVE description: An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers on systems with the speakup driver could cause a local denial of service attack, aka CID-d41227544427. This occurs because of an invalid free when the line discipline is used more than once.

- Problem Type:
  - CWE-763
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 5.5 (Medium)

5.5 CVE-2020-29568

An issue in Xen through 4.14.x, which affects all systems with Linux was discovered which might trigger an OOM in the back-end.

CVE description: An issue was discovered in Xen through 4.14.x. Some OSes (such as Linux, FreeBSD, and NetBSD) are processing watch events using a single thread. If the events are received faster than the thread is able to handle, they will get queued. As the queue is unbounded, a guest may be able to trigger an OOM in the backend. All systems with a FreeBSD, Linux, or NetBSD (any version) dom0 are vulnerable.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

5.6 CVE-2020-29569

Issue discovered in the Linux kernel can allow an attacker to crash the system. Privilege escalation and information leaks cannot be ruled out.

CVE description: An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblkd to NULL when stopped. However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a dom0 crash by continuously connecting / disconnecting a block frontend. Privilege escalation and information leaks cannot be ruled out. This only affects systems with a Linux blkback.

- Problem Type:
  - CWE-252
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.7 CVE-2020-29660

A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.

CVE description: A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.

- Problem Type:
  - CWE-416
  - CWE-667
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 4.4 (Medium)

5.8 CVE-2020-29661

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.

Ubuntu has issued an update for kernel that fixes this and multiple vulnerabilities.

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)

5.9 CVE-2021-20232

A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.

This is fixed in version 3.7.1. or later versions.

CVE description: A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.

- Problem Type:
  - CWE-416
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H
  - Base Score: 7.4 (High)

5.10 CVE-2021-24031

In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties. Ubuntu has issued an update for libzstd that fixes this vulnerability.

CVE description: In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.

- Problem Type:
  - Insecure Inherited Permissions (CWE-277)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
  - Base Score: 9.1 (Critical)

5.11 CVE-2021-24032

An incomplete fix for CVE-2021-24031, can allow output files momentarily be readable or writeable to unintended parties in some Linux based systems.

CVE description: Beginning in v1.4.1 and prior to v1.4.9, due to an incomplete fix for CVE-2021-24031, the Zstandard command-line utility created output files with default permissions and restricted those permissions immediately afterwards. Output files could therefore momentarily be readable or writable to unintended parties.

- Problem Type:
  - Insecure Inherited Permissions (CWE-277)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
  - Base Score: 9.1 (Critical)

5.12 CVE-2021-27218

An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation. Ubuntu has issued an update for glib2.0, which fixes this and other multiple vulnerabilities which can allow causing a DoS.

CVE description: An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation.

- Problem Type:
  - CWE-681
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.13 CVE-2021-27219

An integer overflow issue was discovered in GNOME GLib that could potentially lead to memory corruption.

CVE description: An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.

- Problem Type:
  - CWE-681
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.14 CVE-2021-27803

Vulnerability that could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.

CVE description: A vulnerability was discovered in how p2p/p2p_pd.c in wpa_supplicant before 2.10 processes P2P (Wi-Fi Direct) provision discovery requests. It could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.5 (High)

6 Additional Resources

[1] Bosch Rexroth Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

7 Revision History

23 Apr 2021: Initial Publication