Security Advisory
Multiple vulnerabilities (ctrlX CORE)

1 Advisory Information

Advisory ID: BOSCH-SA-029150

CVE Numbers and CVSS v3.1 Scores:

- CVE-2016-10228
  - Base Score: 5.9 (Medium)
- CVE-2019-25013
  - Base Score: 5.9 (Medium)
- CVE-2020-27618
  - Base Score: 5.5 (Medium)
- CVE-2020-29562
  - Base Score: 4.8 (Medium)
- CVE-2020-6096
  - Base Score: 8.1 (High)
- CVE-2021-27645
  - Base Score: 2.5 (Low)
- CVE-2021-3326
  - Base Score: 7.5 (High)
- CVE-2021-35942
  - Base Score: 9.1 (Critical)
- CVE-2021-3998
  - Base Score: n/a
- CVE-2021-3999
  - Base Score: n/a
- CVE-2021-45960
  - Base Score: 8.8 (High)
- CVE-2021-46143
  - Base Score: 8.1 (High)
- CVE-2022-0778
  - Base Score: 7.5 (High)
- CVE-2022-22822
  - Base Score: 9.8 (Critical)
- CVE-2022-22823
  - Base Score: 9.8 (Critical)
- CVE-2022-22824
  - Base Score: 9.8 (Critical)
- CVE-2022-22825
  - Base Score: 8.8 (High)
- CVE-2022-22826
  - Base Score: 8.8 (High)
- CVE-2022-22827
  - Base Score: 8.8 (High)
- CVE-2022-23218
  - Base Score: 9.8 (Critical)

- CVE-2022-23219
  - Base Score: 9.8 (Critical)
- CVE-2022-23852
  - Base Score: 9.8 (Critical)
- CVE-2022-23990
  - Base Score: 9.8 (Critical)
- CVE-2022-25235
  - Base Score: 9.8 (Critical)
- CVE-2022-25236
  - Base Score: 9.8 (Critical)

Published: 20 Apr 2022
Last Updated: 20 Apr 2022

2 Summary

The base operating system app core20, which is part of ctrlX CORE XCR (base system apps), includes vulnerable versions of expat, libc and OpenSSL. Furthermore, multiple ctrlX CORE apps use at least one of the libraries shipped with core20. An attacker might be able to escalate privileges, gain system access or cause a denial of service of the device by successfully exploiting one of the vulnerabilities.
The Node-Red app includes a vulnerable version of Node.js, which is affected by the OpenSSL vulnerability. A successful exploitation might allow an attacker to cause a denial of service.

3 Affected Products

- ctrlX CORE < XCR-V-0114.1
  - CVE-2016-10228
  - CVE-2019-25013
  - CVE-2020-27618
  - CVE-2020-29562
  - CVE-2020-6096
  - CVE-2021-27645
  - CVE-2021-3326
  - CVE-2021-35942
  - CVE-2021-3998
  - CVE-2021-3999
  - CVE-2021-45960
  - CVE-2021-46143
  - CVE-2022-0778
  - CVE-2022-22822
  - CVE-2022-22823
  - CVE-2022-22824
  - CVE-2022-22825
  - CVE-2022-22826
  - CVE-2022-22827
  - CVE-2022-23218
  - CVE-2022-23219
  - CVE-2022-23852
  - CVE-2022-23990
  - CVE-2022-25235
  - CVE-2022-25236

- ctrlX CORE (LTS) < XCR-V-0112.15
  - CVE-2016-10228
  - CVE-2019-25013
  - CVE-2020-27618
  - CVE-2020-29562
  - CVE-2020-6096
  - CVE-2021-27645
  - CVE-2021-3326
  - CVE-2021-35942
  - CVE-2021-3998
  - CVE-2021-3999
  - CVE-2021-45960
  - CVE-2021-46143
  - CVE-2022-0778
  - CVE-2022-22822
  - CVE-2022-22823
  - CVE-2022-22824
  - CVE-2022-22825
  - CVE-2022-22826
  - CVE-2022-22827
  - CVE-2022-23218
  - CVE-2022-23219
  - CVE-2022-23852
  - CVE-2022-23990
  - CVE-2022-25235
  - CVE-2022-25236
- ctrlX CORE (Node-Red) < RED-V-0114.4
  - CVE-2022-0778
- ctrlX CORE (Node-Red) (LTS) < RED-V-0112.4
  - CVE-2022-0778

4 Solution

4.1 Update to the latest released versions

Updated versions of core20 (as part of XCR) and Node-Red (RED) are available. The user is strongly advised to update to the latest versions:

- core20 20220318 (part of XCR-V-0112.15)
- RED-V-0112.4 (LTS branch)
- core20 20220318 (part of XCR-V-0114.1)
- RED-V-0114.4

The update of core20 might require a reboot of the device and the device will therefore temporarily become unavailable. To verify that the updated versions are installed, please check the version by using the package management of the device.

4.2 Compensatory Measures

The vulnerabilities cannot be exploited remotely without prior authentication.

To exploit the vulnerabilities, an attacker must be logged in on the device. Additionally, the attacker must be permitted to use at least one of the installed apps on the device (this is usually the case). Therefore, only assign permissions following the "Least-Privilege" principle.

Due to the high severity rating of the vulnerabilities, it is strongly advised to use up-to-date versions of the affected apps.

5 Vulnerability Details

5.1 CVE-2016-10228

CVE description: The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.

- Problem Type:
  - CWE-20
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 5.9 (Medium)

5.2 CVE-2019-25013

CVE description: The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.

- Problem Type:
  - CWE-125
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 5.9 (Medium)

5.3 CVE-2020-27618

CVE description: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.

- Problem Type:
  - CWE-835
- 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)

5.4 CVE-2020-29562

CVE description: The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

- Problem Type:
  - CWE-617
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H
  - Base Score: 4.8 (Medium)

5.5 CVE-2020-6096

CVE description: An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

- Problem Type:
  - CWE-191
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

5.6 CVE-2021-27645

CVE description: The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.

- Problem Type:
  - CWE-415
- CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
  - Base Score: 2.5 (Low)

5.7 CVE-2021-3326

CVE description: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

- Problem Type:
  - CWE-617
- 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)

5.8 CVE-2021-35942

CVE description: The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
  - Base Score: 9.1 (Critical)

5.9 CVE-2021-3998

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.

- CVSS Vector String: n/a

5.10 CVE-2021-3999

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.

- CVSS Vector String: n/a

5.11 CVE-2021-45960

CVE description: In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).

- Problem Type:
  - CWE-400
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.12 CVE-2021-46143

CVE description: In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AC:H/AV:N/A:H/C:H/I:H/PR:N/S:U/UI:N
  - Base Score: 8.1 (High)

5.13 CVE-2022-0778

CVE description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Problem Type:
  - CWE-835
- 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-2022-22822

CVE description: addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.15 CVE-2022-22823

CVE description: build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.16 CVE-2022-22824

CVE description: defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.17 CVE-2022-22825

CVE description: lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.18 CVE-2022-22826

CVE description: nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.19 CVE-2022-22827

CVE description: storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.20 CVE-2022-23218

CVE description: The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

- Problem Type:
  - CWE-120
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.21 CVE-2022-23219

CVE description: The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

- Problem Type:
  - CWE-120
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.22 CVE-2022-23852

CVE description: Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.23 CVE-2022-23990

CVE description: Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function.

- Problem Type:
  - CWE-190
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.24 CVE-2022-25235

CVE description: xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.

- Problem Type:
  - CWE-116
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.25 CVE-2022-25236

CVE description: xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.

- Problem Type:
  - CWE-668
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

6 Additional Resources

[1] Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/de/de/myrexroth/media-directory-download?object_nr=R911342562

7 Revision History

20 Apr 2022: Initial Publication