# Security Advisory
## ctrlX CORE - IDE App affected by OpenSSL and Python Vulnerabilities

## 1 Advisory Information

**Advisory ID: BOSCH-SA-017743**
**CVE Numbers and CVSS v3.1 Scores:**

- CVE-2020-26116
  - Base Score: 7.2 (High)
- CVE-2020-27619
  - Base Score: 9.8 (High)
- CVE-2021-23336
  - Base Score: 5.9 (Medium)
- CVE-2021-23840
  - Base Score: 7.5 (High)
- CVE-2021-23841
  - Base Score: 5.9 (Medium)
- CVE-2021-3177
  - Base Score: 9.8 (High)
- CVE-2021-3449
  - Base Score: 5.9 (Medium)

**Published:** 30 Apr 2021
**Last Updated:** 30 Apr 2021

## 2 Summary

Multiple vulnerabilities affecting OpenSSL Versions previous to 1.1.1k and Python 0 through 3.9.1, have been reported. Affected versions are included in the ctrlX CORE- IDE App. In order to successfully exploit these vulnerabilities, an attacker requires access to the network or system. Two vulnerabilities (CVE-2021-3177 and CVE-2021-27619) are notably critical, as they can be easily exploited. The exploitation of these vulnerabilities can lead to remote code execution (CVE-2021-3177, CVE-27619), unexpected communication behavior (CVE-2021-2336, CVE-2020-26116), crash and Denial of Service (CVE-2021-3449, CVE-2021-23841, CVE-2021-23840, CVE-27619).

The affected functions of the aforementioned vulnerabilities are not used directly by the ctrlX CORE - IDE App and hence, the exploitation risk is low. Nonetheless, vulnerable versions of these components are included and it cannot be completely ruled out that these functions might be indirectly called. For this reason, Bosch Rexroth recommends to update the affected product to their latest version.

These vulnerabilities do not affect the ctrlX CORE Runtime.

## 3 Affected Products

- ctrlX CORE - IDE App <= 1.8.0

# 4 Solutions and Mitigations

## 4.1 Software Update

The next release of the ctrlX CORE - IDE App includes updated versions of OpenSSL and Python. It is strongly recommended that customers update all previous instances using prior versions once it is made available. Please contact your sales partner for instructions on how to retrieve these 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.

If an update is not possible in a timely manner, please implement the compensatory measures described below.

## 4.2 Compensatory Measures

Bosch Rexroth strongly recommends to operate the ctrlX CORE - IDE App in a closed network with no internet access and to implement appropriate security measures such as those described in the “Security Guideline Electric Drives and Controls” [1], for example network segmentation.

Moreover, it is strongly recommended that only select users are granted the required permissions to use the ctrlX CORE - IDE App.

# 5 Vulnerability Details

## 5.1 CVE-2020-26116

CVE description: http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.

- Problem Type:
  - CWE-116
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
  - Base Score: 7.2 (High)

## 5.2 CVE-2020-27619

CVE description: In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP.

- Problem Type:
  - n/a
- 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)

## 5.3 CVE-2021-23336

CVE description: The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.0 and before 3.9.2 are vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.

- Problem Type:
  - CWE-444
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H/E:P/RL:U/RC:C
  - Base Score: 5.9 (Medium)

## 5.4 CVE-2021-23840

CVE description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Problem Type:
  - CWE-190
- 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)

## 5.5 CVE-2021-23841

CVE description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Problem Type:
  - CWE-190
- 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)

## 5.6 CVE-2021-3177

CVE description: Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

- 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)

### 5.7 CVE-2021-3449

CVE description: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- Problem Type:
  - CWE-476
- 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)

# 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

30 Apr 2021: Initial Publication