Security Advisory

1 ctrlX Products affected by OpenSSL Vulnerability CVE-2020-1971

2 Advisory Information

Advisory ID: BOSCH-SA-274557
CVE Numbers and CVSS v3.1 Scores:

- CVE-2020-1971
  - Base Score: 5.9 (Medium)

Published: 18 Dec 2020
Last Updated: 21 Jan 2021

3 Summary

The OpenSSL Software Foundation has published information [1] for OpenSSL versions prior to 1.1.1i (1.1.1 – 1.1.1h) and 1.0.2x (1.0.2 – 1.0.2w) regarding a weakness in the *GENERAL_NAME_cmp* function. The vulnerability could allow an attacker to provoke a null pointer dereference, potentially leading to a denial of service.
Multiple components of Bosch Rexroth are shipped with a vulnerable OpenSSL version.
The aforementioned function is 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 function might be called indirectly. It is therefore strongly advised to follow the suggested solution and mitigations.

4 Affected Products

- ctrlX CORE Runtime < XCR-V-0106.1
- ctrlX CORE OPC UA Server < UAS-V-0106.1
- ctrlX CORE OPC UA Client < UAC-V-0106.3
- ctrlX WORKS < V0106.1

5 Solution and Mitigations

5.1 Software Update

For ctrlX CORE (+ the affected components) an updated release is available. 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.
The next release of ctrlX WORKS will include a patch as well. It is recommended to update ctrlX WORKS as soon as the update becomes available.

5.2 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 [2]). In general, it is highly recommended to implement the measures described in the “Security Guideline Electric Drives and Controls”.

6 Vulnerability Details

6.1 CVE-2020-1971

ctrlX products are shipped with OpenSSL versions vulnerable to CVE-2020-1971.

CVE description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL’s s_server, s_client and verify tools have support for the “-crl_download” option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL’s parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- Problem Type:
  - NULL pointer dereference
- 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)

7 Additional Resources

[1] https://www.openssl.org/news/secadv/20201208.txt
[2] Bosch Rexroth Security Guideline Electric Drives and Controls: https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

8 Revision History

21 Jan 2021: Update 4 Affected Products and 5.1 Software Update
18 Dec 2020: Initial Publication