Security Advisory

Multiple vulnerabilities on ctrlX HMI / WR21

1 Advisory Information

Advisory ID: BOSCH-SA-175607

CVE Numbers and CVSS v3.1 Scores:

- CVE-2023-41255
  - Base Score: 8.8 (High)
- CVE-2023-41372
  - Base Score: 7.8 (High)
- CVE-2023-41960
  - Base Score: 7.1 (High)
- CVE-2023-43488
  - Base Score: 7.9 (High)
- CVE-2023-45220
  - Base Score: 8.8 (High)
- CVE-2023-45321
  - Base Score: 8.3 (High)
- CVE-2023-45844
  - Base Score: 7.3 (High)
- CVE-2023-45851
  - Base Score: 8.8 (High)
- CVE-2023-46102
  - Base Score: 8.8 (High)

Published: 20 Oct 2023

Last Updated: 21 Nov 2023

2 Summary

The operating system of the ctrlX HMI/ WR21 before build date 20231107 has some vulnerabilities when the kiosk mode is used in conjunction with Google Chrome. Therefore, it is possible in worst case that an attacker with physical access to the device can get root access without normal authentication borders.

Additionally, the "Android Agent" application which is an onboard application of ctrlX HMI/ WR21 before build date 20231107 contains some weaknesses regarding the execution of arbitrary commands on the device. All weaknesses were eliminated in the newest firmware version which can be updated on the existing devices.

3 Affected Products

- ctrlX HMI / WR21 (WR2107) < RC7 (Build date 20231107)
- ctrlX HMI / WR21 (WR2110) < RC7 (Build date 20231107)
- ctrlX HMI / WR21 (WR2115) < RC7 (Build date 20231107)

4 Solution

An updated firmware version is available. This version prevents that an attacker with physical access to the device might gain root access.

Furthermore, the application "Android Agent" will be removed entirely.

Please contact your sales partner for instructions on how to retrieve the update. Users are strongly advised to upgrade to the new version.

5 Mitigation

Until the updated version is installed, users are strongly advised not to use Google Chrome for the Kiosk mode. As an alternative, the WebStation app may be used for this purpose.

Android Agent should not be used at all.

6 Vulnerability Details

6.1 CVE-2023-41255

CVE description: The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the ‘su’ binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network.

- Problem Type:
  - CWE-306 Missing Authentication for Critical Function
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

6.2 CVE-2023-41372

CVE description: The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server. This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair.

- Problem Type:
  - CWE-798 Use of Hard-coded Credentials
- 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)

6.3 CVE-2023-41960

CVE description: The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself.

- Problem Type:
  - CWE-926 Improper Export of Android Application Components
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
  - Base Score: 7.1 (High)

6.4 CVE-2023-43488

CVE description: The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB.

- Problem Type:
  - CWE-862 Missing Authorization
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L
  - Base Score: 7.9 (High)

6.5 CVE-2023-45220

CVE description: The Android Client application, when enrolled with the define method 1(the user manually inserts the server IP address), use HTTP protocol to retrieve sensitive information (IP address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user.

- Problem Type:
  - CWE-306 Missing Authentication for Critical Function
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

6.6 CVE-2023-45321

CVE description: The Android Client application, when enrolled with the define method 1 (the user manually inserts the server IP address), use HTTP protocol to retrieve sensitive information (IP address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP, this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol.

- Problem Type:
  - CWE-319 Cleartext Transmission of Sensitive Information
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
  - Base Score: 8.3 (High)

6.7 CVE-2023-45844

CVE description: The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug).

- Problem Type:
  - CWE-284 Improper Access Control
- CVSS Vector String: CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
  - Base Score: 7.3 (High)

6.8 CVE-2023-45851

CVE description: The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker without enforcing any server authentication.

This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device.

- Problem Type:
  - [CWE-306 Missing Authentication for Critical Function]
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

6.9 CVE-2023-46102

CVE description: The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages, and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application.

This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself.

- Problem Type:
  - CWE-798 Use of Hard-coded Credentials
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

7 Remarks

7.1 Acknowledgement

The vulnerability has been uncovered and disclosed responsibly by **Diego Giubertoni** from **Nozomi Networks**. We thank him for making a responsible disclosure with us.

8 Revision History

21 Nov 2023: Update as patch is available
25 Oct 2023: Added CVE list
20 Oct 2023: Initial Publication