Security Advisory

Vulnerabilities in ctrlX OS - Setup

1 Advisory Information

Advisory ID: BOSCH-SA-129652
CVE Numbers and CVSS v3.1 Scores:

- CVE-2025-48860
  - Base Score: 8.0 (High)
- CVE-2025-48861
  - Base Score: 5.3 (Medium)
- CVE-2025-48862
  - Base Score: 7.1 (High)

Published: 14 Aug 2025
Last Updated: 14 Aug 2025

2 Summary

The base ctrlX OS Setup app contains multiple vulnerabilities. In a worst case scenario, an authenticated (low privileged) attacker to gain remote access to backup archives created by a user with elevated permissions. Depending on the content of the backup archive, the attacker may have been able to access sensitive data.

3 Affected Products

- ctrlX OS - Setup
  - CVE-2025-48860, CVE-2025-48861, CVE-2025-48862
    - Version(s): 1.20.0 <= 1.20.1
    - Version(s): 2.6.0 <= 2.6.1
    - Version(s): 3.6.0 <= 3.6.2

4 Solution

4.1 Update

An updated version of the affected component is available for all long term supported (LTS) releases. The user is strongly recommended to update to the latest version. The update of the app might require a reboot of the device, and the device will therefore temporarily become unavailable. To verify that the updated version is installed, please check the version by using the package management of the device.

4.2 Compensatory Measures

For the following vulnerabilities, countermeasures exist which mitigate the risk:

- CVE-2025-48860:
  When a backup has been created and downloaded, delete the created backup file using the web interface.

- CVE-2025-48862:
  When encryption is required for the files contained in the backup, use an external program to encrypt the backup file after the download.

Nevertheless, it is strongly advised to use an up-to-date version of the affected app.

5 Vulnerability Details

5.1 CVE-2025-48860

CVE description: A vulnerability in the web application of the ctrlX OS setup mechanism facilitated an authenticated (low privileged) attacker to gain remote access to backup archives created by a user with elevated permissions. Depending on the content of the backup archive, the attacker may have been able to access sensitive data.

- Problem Type:
  - CWE-284 Improper Access Control
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.0 (High)

5.2 CVE-2025-48861

CVE description: A vulnerability in the Task API endpoint of the ctrlX OS setup mechanism allowed a remote, unauthenticated attacker to access and extract internal application data, including potential debug logs and the version of installed apps.

- Problem Type:
  - CWE-284 Improper Access Control
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 5.3 (Medium)

5.3 CVE-2025-48862

CVE description: Ambiguous wording in the web interface of the ctrlX OS setup mechanism could lead the user to believe that the backup file is encrypted when a password is set. However, only the private key - if available in the backup - is encrypted, while the backup file itself remains unencrypted.

- Problem Type:
  - CWE-1104 Use of Unmaintained Third Party Components
  - CWE-311 Missing Encryption of Sensitive Data
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
  - Base Score: 7.1 (High)

6 Remarks

6.1 Acknowledgement

The vulnerabilities have been uncovered and disclosed responsibly by **Michael Messner** and **Benedikt Kuehne** from **Siemens Energy**. We thank them for making a responsible disclosure with us.

6.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

7 Additional Resources

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

8 Revision History

14 Aug 2025: Initial Publication