Security Advisory
Multiple ctrlX OS vulnerabilities

1 Advisory Information

Advisory ID: BOSCH-SA-640452
CVE Numbers and CVSS v3.1 Scores:

- CVE-2025-24338
  - Base Score: 7.1 (High)
- CVE-2025-24339
  - Base Score: 5.0 (Medium)
- CVE-2025-24340
  - Base Score: 6.5 (Medium)
- CVE-2025-24341
  - Base Score: 6.5 (Medium)
- CVE-2025-24342
  - Base Score: 5.3 (Medium)
- CVE-2025-24343
  - Base Score: 5.4 (Medium)
- CVE-2025-24344
  - Base Score: 6.3 (Medium)
- CVE-2025-24345
  - Base Score: 6.3 (Medium)
- CVE-2025-24346
  - Base Score: 7.5 (High)
- CVE-2025-24347
  - Base Score: 6.5 (Medium)
- CVE-2025-24348
  - Base Score: 5.4 (Medium)
- CVE-2025-24349
  - Base Score: 7.1 (High)
- CVE-2025-24350
  - Base Score: 7.1 (High)
- CVE-2025-24351
  - Base Score: 8.8 (High)
- CVE-2025-27532
  - Base Score: 6.5 (Medium)

Published: 25 Apr 2025
Last Updated: 28 Apr 2025

2 Summary

The base ctrlX OS apps Device Admin and Solutions contain multiple vulnerabilities. In a worst case scenario, a remote authenticated (low-privileged) attacker might be able to execute arbitrary OS commands running with higher privileges. The vulnerabilities have been uncovered and disclosed responsibly by Nozomi. We thank them for making a responsible disclosure with us.

3 Affected Products

- Bosch Rexroth AG ctrlX OS - Device Admin
  - CVE-2025-24339, CVE-2025-24340, CVE-2025-24341, CVE-2025-24342, CVE-2025-24346, CVE-2025-24347, CVE-2025-24348, CVE-2025-24349, CVE-2025-24350
    - Version(s): 1.12.0 < 1.12.10
    - Version(s): 1.20.0 < 1.20.8
    - Version(s): 2.6.0 < 2.6.9
  - CVE-2025-24345, CVE-2025-24351
    - Version(s): 1.20.0 < 1.20.8
    - Version(s): 2.6.0 < 2.6.9
  - CVE-2025-27532
    - Version(s): 1.12.0 < 1.12.10
    - Version(s): 1.20.0 < 1.20.8
- Bosch Rexroth AG ctrlX OS - Solutions
  - CVE-2025-24338, CVE-2025-24343, CVE-2025-24344
    - Version(s): 1.12.0 < 1.12.2
    - Version(s): 1.20.0 < 1.20.2
    - Version(s): 2.6.0

4 Solution

4.1 Update

Updated versions of the affected components are available for all LTS releases. The user is strongly recommended to update to the latest versions. The update of the apps 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 affected by

- CVE-2025-24338
- CVE-2025-24340
- CVE-2025-24341
- CVE-2025-24343
- CVE-2025-24345
- CVE-2025-24346
- CVE-2025-24347
- CVE-2025-24348
- CVE-2025-24349
- CVE-2025-24350
- CVE-2025-24351
- CVE-2025-27352

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 affected functionalities on the device. Therefore, only assign permissions following the "Least-Privilege" principle. Additionally, make sure that for all user accounts strong password policies are enforced. The default password policies of ctrlX OS are considered as sufficiently strong.

For the following CVEs, please apply individual measures:

- CVE-2025-24339: Make sure that all links are verified before clicking them and always access ctrlX OS using the secure https address, only
- CVE-2025-24342: Make sure that for all user accounts strong password policies are set so that even when an attacker is able to determine that a specific account exists, brute-forcing the password is not feasible
- CVE-2025-24344: Make sure that artefacts are coming from a trustworthy source before uploading them to ctrlX OS

Nevertheless, it is strongly advised to use up-to-date versions of the affected apps.

5 Vulnerability Details

5.1 CVE-2025-24338

CVE description: A vulnerability in the “Manages app data” functionality of the web application of ctrlX OS allows a remote authenticated (lowprivileged) attacker to execute arbitrary client-side code in the context of another user’s browser via multiple crafted HTTP requests.

- Problem Type:
  - CWE-116 Improper Encoding or Escaping of Output
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.1 (High)

5.2 CVE-2025-24339

CVE description: A vulnerability in the web application of ctrlX OS allows a remote unauthenticated attacker to conduct various attacks against users of the vulnerable system, including web cache poisoning or Man-in-the-Middle (MitM), via a crafted HTTP request.

- Problem Type:
  - CWE-644 Improper Neutralization of HTTP Headers for Scripting Syntax
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.0 (Medium)

5.3 CVE-2025-24340

CVE description: A vulnerability in the users configuration file of ctrlX OS may allow a remote authenticated (low-privileged) attacker to recover the plaintext passwords of other users.

- Problem Type:
  - CWE-916 Use of Password Hash With Insufficient Computational Effort
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

5.4 CVE-2025-24341

CVE description: A vulnerability in the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to induce a Denial-of-Service (DoS) condition on the device via multiple crafted HTTP requests. In the worst case, a full power cycle is needed to regain control of the device.

- Problem Type:
  - CWE-770 Allocation of Resources Without Limits or Throttling
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

5.5 CVE-2025-24342

CVE description: A vulnerability in the login functionality of the web application of ctrlX OS allows a remote unauthenticated attacker to guess valid usernames via multiple crafted HTTP requests.

- Problem Type:
  - CWE-204 Observable Response Discrepancy
- 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)

5.6 CVE-2025-24343

CVE description: A vulnerability in the “Manages app data” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to write arbitrary files in arbitrary file system paths via a crafted HTTP request.

- Problem Type:
  - CWE-23 Relative Path Traversal
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
  - Base Score: 5.4 (Medium)

5.7 CVE-2025-24344

CVE description: A vulnerability in the error notification messages of the web application of ctrlX OS allows a remote unauthenticated attacker to inject arbitrary HTML tags and, possibly, execute arbitrary client-side code in the context of another user’s browser via a crafted HTTP request.

- Problem Type:
  - CWE-81 Improper Neutralization of Script in an Error Message Web Page
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 6.3 (Medium)

5.8 CVE-2025-24345

CVE description: A vulnerability in the “Hosts” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to manipulate the “hosts” file in an unintended manner via a crafted HTTP request.

- Problem Type:
  - CWE-1286 Improper Validation of Syntactic Correctness of Input
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 6.3 (Medium)

5.9 CVE-2025-24346

CVE description: A vulnerability in the “Proxy” functionality of the web application of ctrlX OS allows a remote authenticated (lowprivileged) attacker to manipulate the “/etc/environment” file via a crafted HTTP request.

- Problem Type:
  - CWE-1286 Improper Validation of Syntactic Correctness of Input
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.5 (High)

5.10 CVE-2025-24347

CVE description: A vulnerability in the “Network Interfaces” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to manipulate the network configuration file via a crafted HTTP request.

- Problem Type:
  - CWE-1286 Improper Validation of Syntactic Correctness of Input
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

5.11 CVE-2025-24348

CVE description: A vulnerability in the “Network Interfaces” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to manipulate the wireless network configuration file via a crafted HTTP request.

- Problem Type:
  - CWE-1286 Improper Validation of Syntactic Correctness of Input
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
  - Base Score: 5.4 (Medium)

5.12 CVE-2025-24349

CVE description: A vulnerability in the “Network Interfaces” functionality of the web application of ctrlX OS allows a remote authenticated (lowprivileged) attacker to delete the configuration of physical network interfaces via a crafted HTTP request.

- Problem Type:
  - CWE-183 Permissive List of Allowed Inputs
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
  - Base Score: 7.1 (High)

5.13 CVE-2025-24350

CVE description: A vulnerability in the “Certificates and Keys” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to write arbitrary certificates in arbitrary file system paths via a crafted HTTP request.

- Problem Type:
  - CWE-23 Relative Path Traversal
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
  - Base Score: 7.1 (High)

5.14 CVE-2025-24351

CVE description: A vulnerability in the “Remote Logging” functionality of the web application of ctrlX OS allows a remote authenticated (low-privileged) attacker to execute arbitrary OS commands in the context of user “root” via a crafted HTTP request.

- Problem Type:
  - CWE-78 Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)
- 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)

5.15 CVE-2025-27532

CVE description: A vulnerability in the “Backup & Restore” functionality of the web application of ctrlX OS allows a remote authenticated (lowprivileged) attacker to access secret information via multiple crafted HTTP requests.

- Problem Type:
  - CWE-312 Cleartext Storage of Sensitive Information
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

6 Remarks

6.1 Acknowledgement

These vulnerabilities have been uncovered and disclosed responsibly by **Andrea Palanca** from **Nozomi Networks**. We thank him 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

28 Apr 2025: Update CVSS Score for CVE-2025-27532
25 Apr 2025: Initial Publication