

Security Advisory

Vulnerabilities in Rexroth IndraWorks

1 Advisory Information

Advisory ID: BOSCH-SA-591522

CVE Numbers and CVSS v3.1 Scores:

- ▶ [CVE-2025-60035](#)
 - Base Score: [7.8 \(High\)](#)
- ▶ [CVE-2025-60036](#)
 - Base Score: [7.8 \(High\)](#)
- ▶ [CVE-2025-60037](#)
 - Base Score: [7.8 \(High\)](#)
- ▶ [CVE-2025-60038](#)
 - Base Score: [7.8 \(High\)](#)

Published: 13 Feb 2026

Last Updated: 27 Feb 2026

2 Summary

Trend Micro has identified multiple vulnerabilities in Rexroth IndraWorks which affect both, IndraWorks and utilities that are shipped as part of the package. In a worst case scenario, a successful attack leads to a remote code execution.

3 Affected Products

- ▶ Rexroth IndraWorks
 - CVE-2025-60035, CVE-2025-60036
 - Version(s): < 15V24
 - CVE-2025-60037, CVE-2025-60038
 - Version(s): all
- ▶ Rexroth OPC DA Client
 - CVE-2025-60035
 - Version(s): < v33.0.0.0
- ▶ Rexroth UA.TestClient
 - CVE-2025-60036
 - Version(s): < 2.9.0

4 Solution

4.1 Update

A bugfix for CVE-2025-60035 (OPC DA Client) has been made available in the downloads area of Bosch Rexroth [1].

A bugfix for CVE-2025-60036 (UA.TestClient) has been made available in the Collaboration Rooms of Bosch Rexroth [2].

Users of each application are strongly advised to download the standalone package and to replace the vulnerable version in the IndraWorks installation folder.

IndraWorks 15V24 will be shipped with an OPC DA Client version that is not affected by the vulnerability. Please note that starting with IndraWorks 15V24, UA.TestClient has been removed from the package entirely.

4.2 Compensatory Measures

To maintain backwards compatibility with prior versions of IndraWorks, CVE-2025-60037 and CVE-2025-60038 cannot be resolved. To be affected by this vulnerability, a user must import a file that has been manipulated by an attacker. Therefore, users of IndraWorks are advised to only open and process files from trustworthy sources.

5 Vulnerability Details

5.1 CVE-2025-60035

CVE description: A vulnerability has been identified in the OPC DA Client utility, which is included in Rexroth IndraWorks and available as a separate download. All versions prior to v33.0.0.0 and included in IndraWorks prior to 15V24 are affected. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running the OPC DA Client.

- ▶ Problem Type:
 - [CWE-502 Deserialization of Untrusted Data](#)
- ▶ CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)
 - Base Score: 7.8

5.2 CVE-2025-60036

CVE description: A vulnerability has been identified in the UA.TestClient utility, which is included in Rexroth IndraWorks. All versions prior to 15V24 are affected. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running the UA.TestClient.

- ▶ Problem Type:
 - [CWE-502 Deserialization of Untrusted Data](#)
- ▶ CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)
 - Base Score: 7.8

5.3 CVE-2025-60037

CVE description: A vulnerability has been identified in Rexroth IndraWorks. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running Rexroth IndraWorks.

- ▶ Problem Type:
 - [CWE-502 Deserialization of Untrusted Data](#)
- ▶ CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)
 - Base Score: 7.8

5.4 CVE-2025-60038

CVE description: A vulnerability has been identified in Rexroth IndraWorks. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running Rexroth IndraWorks.

- ▶ Problem Type:
 - [CWE-502 Deserialization of Untrusted Data](#)
- ▶ CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)
 - Base Score: 7.8

6 Remarks

6.1 Acknowledgement

The vulnerabilities have been uncovered and disclosed responsibly by **Trend Micro**. 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 OPC DA Client:
<https://www.boschrexroth.com/de/de/media-details/2f969694-b755-407f-9d02-8f86aee0e98c>

[2] Bosch Rexroth UA.TestClient:
https://www.boschrexroth.com/de/de/myrexroth/collaboration/collaboration-rooms/?path=/CtrlX-Automation/ctrlX_eShop/ctrlX%20CORE%20-%20OPC%20UA%20Apps

8 Revision History

27 Feb 2026: Update as patch is available

13 Feb 2026: Initial Publication