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: 13 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 UA.Testclient
  - CVE-2025-60036
    - Version(s): < 2.9.0

4 Solution

IndraWorks 15V24 will be released on 27.02.2026 and contains fixes for the following CVE:

- CVE-2025-60035
- CVE-2025-60036

For CVE-2025-60037 and CVE-2025-60038 updated versions of IndraWorks will become available later. This advisory will be updated as soon as those versions are available.

Users are strongly advised to update to IndraWorks 15V24 as soon as the updates become available. Please contact your sales partner for instructions on how to retrieve the update.

Starting with IndraWorks 15V24, UA.TestClient (affected by CVE-2025-60036) has been removed from the package entirely. Users of the application are advised to install the standalone package, which is available in the Collaboration Room. UA.TestClient 2.9.0 and higher contain the fixes for CVE-2025-60036.

Until updates become available and for use cases in which updates are not possible, the users 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.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 OPC.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

5.2 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 Revision History

13 Feb 2026: Initial Publication