Product Security Advisory

Vulnerability in Algo Edge (previously-used component of navify® Algorithm Suite)
CVE-2024-13026, CWE-326

Publish Date: 2025-01-15
Last Update: 2025-01-15

Executive Summary

Roche is aware of a vulnerability in Algo Edge - a previously used (legacy) component of navify® Algorithm Suite. The vulnerability impacts the authentication mechanism of this component and could allow an attacker with local access to the laboratory network and the Algo Edge system to craft valid authentication tokens and access the component. Other components of navify® Algorithm Suite are not affected.

Roche Diagnostics has assessed the potential impact from this vulnerability and has released an update of this component and has migrated affected customers to a new solution.

As a general security measure, Roche strongly recommends to thoroughly control network access to devices with appropriate mechanisms including the Roche-provided firewall. We highly recommend configuring the operating environment according to Roche's installation guidelines and to follow the recommendations in the product manuals.

Affected Products

Our current assessment of the reported vulnerability is that all versions of Algo Edge before 2.1.2 are impacted. Almost all customers have already received an updated version of Algo Edge (2.1.2 or higher) or have migrated to the new solution.

Please contact your local Roche Diagnostics office for further information on the update schedule.

Potential Impact

The vulnerability impacts the authentication mechanism of Algo Edge that controls access to a service interface and could allow an attacker with local access to the laboratory network and the Algo Edge system to craft valid authentication tokens and access the component. The weakness is only exposed to the internal authorized laboratory network which is currently protected by existing overall security controls. For this reason, Roche believes the risk is significantly reduced. Additionally, the impacted component only manages transient data.

CVE-2024-13026 (CWE-326)
CVSS v4.0 Score: 5.7 / Medium
CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/S:N/AU:N/R:A/V:D/RE:L/U:Clear

---

Mitigations / Workarounds

No temporary workarounds are necessary as all customers affected have been or are being migrated to the new solution.

Acknowledgments

Roche thanks Calif.io for reporting this vulnerability.

Contact Information

Roche Customers
For further information or concerns, please contact your local Roche Diagnostics office.

Security Researchers
For Diagnostics product-related security topics, please contact product.security@roche.com
For general Roche related security topics, please contact security@roche.com