Product Security Advisory

Vulnerability in navify® Monitoring

CVE-2025-7674, CWE-20

Publish Date: 2025-07-17
Last Update: 2025-07-17

Executive Summary

Roche Diagnostics has recently detected a vulnerability in the input validation mechanism of an API (Application Programming Interface), which lacks adequate validation measures for data input provided by users. Attackers can potentially exploit this vulnerability by sending excessively large sets of data, or unexpected data, with malicious intent to the API. Without proper validation by the software, this flawed input could potentially negatively impact the server's performance, leading to resource exhaustion or saturation. Consequently, the server could consume all available memory, or network connections, or CPU resources resulting in a Denial of Service (DoS) and rendering the API unusable for legitimate users.

After assessing the potential impact of this vulnerability, Roche Diagnostics has implemented updates to rectify the flaw. Roche has also put measures in place to enforce strict input validation, define expected limits and formats for each type of data, utilizing sanitization techniques to strip harmful content, and establishing robust error handling systems to efficiently identify and respond to abnormal traffic patterns.

As a general security measure, Roche strongly recommends thorough control of 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 adhering to recommendations provided in the product manuals.

Affected Products

The reported vulnerability impacts all versions of navify® Monitoring prior to version 1.08.00. The full package with the issue fixed is available via your Roche contact, so customers can be updated to the latest version.

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

Potential Impact

This vulnerability in improper input validation can be exploited by attackers to affect the server's performance adversely, leading to resource exhaustion or saturation. The server may consume all available memory, or network connections, or CPU resources resulting in a Denial of Service (DoS) and rendering the API unusable for legitimate users. The weakened server interface, if accessed maliciously, may have severe consequences such as operational and financial losses and damage to service reputation.

CVE-2025-7674 (CWE-20)
CVSS v4.0 Score: 7.1 / High
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/S:N/AU:Y/R:U/V:D/RE:M/U:Green

---

Mitigations / Workarounds

No temporary workarounds are necessary as all affected customers have been or are currently being migrated to the new solution with strict input validation mechanisms.

For further information or questions, please contact your local Roche Diagnostics representative or office.

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