Product Security Advisory

Vulnerability in navify® Digital Pathology

CVE-2026-9844 , CWE-1392

Publish Date: 05/29/2026

Last Update: 05/29/2026

Executive Summary

Roche Diagnostics has been alerted about a potential security vulnerability involving the RabbitMQ (RMQ) Management interface of navify Digital Pathology, which is configured with default credentials (guest:guest) by default, unless specifically changed during the installation. This configuration, when exposed, could allow unauthorized network-based access to the complete RabbitMQ management dashboard without proper authentication.

The vulnerability exposes a fully functional message broker management interface that handles internal system operations, including job management, metadata services, upload services, and analysis progress tracking. **While no patient data or sensitive information is exposed**, unauthorized access to this interface allows an attacker to manipulate or disrupt these internal data queues. This vulnerability was reported by an external security researcher.

Affected Products

- navify Digital Pathology (formerly: Virtuoso / uPath) 2.0.0 - 2.4.1

Potential Impact

An unauthorized user leveraging the guest account could allow access to non-public but non-critical data. **No sensitive information is exposed through this vulnerability**. Visible data is restricted to internal identification numbers of various backend systems that cannot be directly linked to specific patients or users.

However, the guest user has full ability to delete queues and inject messages into any queues. In a worst case scenario, an attacker could disrupt the flow of data through RMQ. n.While this does not cause data loss or permanent system damage, an attack could halt the active processing of data queues, causing a temporary disruption to operational workflows.

CVE ID: CVE-2026-9844

Category: CWE-1392: Use of Default Credentials

CVSS v4.0 Score: 8.8 (High)

Vector String:
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:L/SA:L/S:N/AU:Y/R:U/V:D/RE:M/U:Green

---

Mitigations

- Immediate action: Change the default password for the guest user from the factory settings to a secure, unique password.
- Network isolation: Deploy navify Digital Pathology strictly within local or private networks. Limit direct public access to the nDP on-prem server to prevent external access to the RabbitMQ dashboard.

For further guidance on securely configuring navify Digital Pathology, refer to the “Software and data security” section of the User Guide and the Security Addendum to Roche Digital Pathology Dx.

Please contact your local Roche Diagnostics representative or office for further information on remediation.

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