

Forum:[Hack Forums](#)

Thread: [Rockwell Automation FactoryTalk DataMosaix Private Cloud](#)

Stanley - January 25, 2026, 9:20 pm

Rockwell Automation FactoryTalk DataMosaix Private Cloud

View CSAF

Summary

Successful exploitation of this vulnerability could allow an attacker to perform unauthorized sensitive database operations.

The following versions of Rockwell Automation FactoryTalk DataMosaix Private Cloud are affected:

FactoryTalk DataMosaix Private Cloud (CVE-2025-12807)

FactoryTalk DataMosaix Private Cloud (CVE-2025-12807)

FactoryTalk DataMosaix Private Cloud (CVE-2025-12807)

CVSS

Vendor

Equipment

Vulnerabilities

v3 8.8

Rockwell Automation

Rockwell Automation FactoryTalk DataMosaix Private Cloud

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: United States

Vulnerabilities

Expand All +

CVE-2025-12807

A security issue was discovered in DataMosaix Private Cloud, allowing users with low privilege to perform sensitive database operations through exposed Application Programming Interface (API) endpoints.

View CVE Details

Affected Products

Rockwell Automation FactoryTalk DataMosaix Private Cloud

Vendor:Rockwell Automation

Product Version:Rockwell Automation FactoryTalk DataMosaix Private Cloud: 7.11, Rockwell Automation FactoryTalk DataMosaix Private Cloud: 8.00, Rockwell Automation FactoryTalk DataMosaix Private Cloud: 8.01

Product Status:known_affected

Remediations

MitigationRockwell Automation encourages users of the affected software to apply the following risk mitigations, if possible:

Vendor fixUpdate FactoryTalk DataMosaix Private Cloud to Version 8.01.02 or later.

MitigationUsers using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automation's best security practices.

Relevant CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

8.8

HIGH

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Acknowledgments

Rockwell Automation reported this vulnerability to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov/ics](https://www.cisa.gov/ics). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov/ics](https://www.cisa.gov/ics) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

Revision History

Initial Release Date: 2026-01-13

Date
Revision
Summary

2026-01-13

1

Initial republication of Rockwell Automation advisory 'FactoryTalk DataMosaix Private Cloud SQL Injection'

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-013-02>