

# Forum:[Hack Forums](#)

Thread: [Rockwell Automation Verve Asset Manager](#)

Stanley - February 3, 2026, 4:05 pm

Rockwell Automation Verve Asset Manager

View CSAF

Summary

Successful exploitation of these vulnerabilities may allow an attacker to access sensitive information stored in variables within the ADI server.

The following versions of Rockwell Automation Verve Asset Manager are affected:

- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)
- Verve Asset Manager (CVE-2025-14376, CVE-2025-14377)

CVSS

Vendor

Equipment

Vulnerabilities

v3 7.9

Rockwell Automation

Rockwell Automation Verve Asset Manager

Insecure Storage of Sensitive Information, Cleartext Storage of Sensitive Information

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: United States

Vulnerabilities

Expand All +

CVE-2025-14376

A security issue was discovered within the legacy ADI server component of Verve Asset Manager, where unencrypted sensitive data was stored in environment variables. This component was retired and became optional beginning with the 1.36 release in 2024.  
[View CVE Details](#)

Affected Products

Rockwell Automation Verve Asset Manager

Vendor:Rockwell Automation

Product Version:Rockwell Automation Verve Asset Manager: 1.33, Rockwell Automation Verve Asset Manager: 1.34, Rockwell Automation Verve Asset Manager: 1.35, Rockwell Automation Verve Asset Manager: 1.36, Rockwell Automation Verve Asset Manager: 1.37, Rockwell Automation Verve Asset Manager: 1.38, Rockwell Automation Verve Asset Manager: 1.39, Rockwell Automation Verve Asset Manager: 1.40, Rockwell Automation Verve Asset Manager: 1.41, Rockwell Automation Verve Asset Manager: 1.41.1, Rockwell Automation Verve Asset Manager: 1.41.2, Rockwell Automation Verve Asset Manager: 1.41.3  
Product Status:known\_affected

Remediations

MitigationRockwell Automation reports that the issue was resolved in version 1.42, and the component has been optional since version 1.36. Rockwell Automation recommends updating to the latest available version.  
MitigationFor additional details, refer to the advisory on the Rockwell Automation security page.  
MitigationFor further assistance, contact Rockwell Automation TechConnect for help.

Relevant CWE: CWE-922 Insecure Storage of Sensitive Information

Metrics

CVSS Version  
Base Score  
Base Severity  
Vector String

3.1  
7.2  
HIGH

CVE-2025-14377

A security issue was discovered within the legacy Ansible playbook component of Verve Asset Manager. The issue occurred because unencrypted sensitive information was incorrectly stored during playbook execution. This component was retired and became optional starting with the 1.36 release in 2024.  
[View CVE Details](#)

Affected Products  
Rockwell Automation Verve Asset Manager

Vendor:Rockwell Automation  
Product Version:Rockwell Automation Verve Asset Manager: 1.33, Rockwell Automation Verve Asset Manager: 1.34, Rockwell Automation Verve Asset Manager: 1.35, Rockwell Automation Verve Asset Manager: 1.36, Rockwell Automation Verve Asset Manager: 1.37, Rockwell Automation Verve Asset Manager: 1.38, Rockwell Automation Verve Asset Manager: 1.39, Rockwell Automation Verve Asset Manager: 1.40, Rockwell Automation Verve Asset Manager: 1.41, Rockwell Automation Verve Asset Manager: 1.41.1, Rockwell Automation Verve Asset Manager: 1.41.2, Rockwell Automation Verve Asset Manager: 1.41.3  
Product Status:known\_affected

Remediations  
MitigationRockwell Automation reports that the issue was resolved in version 1.42, and the component has been optional since version 1.36. Rockwell Automation recommends updating to the latest available version.  
MitigationFor additional details, refer to the advisory on the Rockwell Automation security page.  
MitigationFor further assistance, contact Rockwell Automation TechConnect for help.

Relevant CWE: CWE-312 Cleartext Storage of Sensitive Information

Metrics

CVSS Version  
Base Score  
Base Severity  
Vector String

## Acknowledgments

Rockwell Automation reported these vulnerabilities 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 these vulnerabilities, 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.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open attachments in unsolicited email messages.

- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

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

## Revision History

Initial Release Date: 2026-01-20

Date  
Revision  
Summary

2026-01-20

1

Initial Republication of Rockwell Automation's security advisory

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-020-03>