

Forum:[Hack Forums](#)

Thread: [Rockwell Automation AADvance-Trusted SIS Workstation](#)

Stanley - November 20, 2025, 4:55 am

Rockwell Automation AADvance-Trusted SIS Workstation

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 8.6

ATTENTION: Exploitable remotely/low attack complexity

Vendor: Rockwell Automation

Equipment: AADvance-Trusted SIS Workstation

Vulnerability: Path Traversal

2. RISK EVALUATION

Successful exploitation of this vulnerability may allow remote code execution.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Rockwell Automation reports the following versions of AADvance-Trusted SIS Workstation, a software suite for developing and managing safety instrumented system (SIS) applications, are affected:

AADvance-Trusted SIS Workstation: Versions 2.00.00 to 2.00.04

3.2 VULNERABILITY OVERVIEW

3.2.1 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-22

A directory traversal vulnerability in DotNetZip v.1.16.0 and earlier may allow a remote attacker to execute arbitrary code via the src/Zip.Shared/ZipEntry.Extract.cs component. Exploitation requires the victim to open a malicious file.

CVE-2024-48510 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48510. A base score of 8.6 has been calculated; the CVSS vector string is

(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United States

3.4 RESEARCHER

Rockwell Automation reported this vulnerability to CISA.

4. MITIGATIONS

Rockwell Automation reports this issue is corrected in software Version 2.01.00 and later.

For more information about this issue, see the advisory on the Rockwell Automation security page. Users of the affected software who are unable to upgrade to one of the corrected versions should follow Rockwell Automation security best practices.

If you have any questions regarding the security issue above and how to mitigate it, contact

TechConnect for assistance. More information can be found at [Contact Us | Rockwell Automation | US](#).

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. 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 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.

5. UPDATE HISTORY

November 13, 2025: Initial Republication of Rockwell Automation

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-10>