

Forum:[Hack Forums](#)

Thread: [Rockwell Automation Studio 5000 Simulation Interface](#)

Stanley - November 25, 2025, 5:35 am

Rockwell Automation Studio 5000 Simulation Interface

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 9.3

ATTENTION: Low attack complexity

Vendor: Rockwell Automation

Equipment: Studio 5000 Simulation Interface

Vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Server-Side Request Forgery (SSRF)

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow attackers to trigger outbound SMB requests to capture NTLM hashes and execute scripts with Administrator privileges upon system reboot.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Rockwell Automation Studio 5000 Simulation Interface are affected:

Studio 5000 Simulation Interface: Version 2.02 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL') CWE-22

A local code execution security issue exists within Studio 5000 Simulation Interface via the API. This vulnerability allows any Windows user on the system to extract files using path traversal sequences, resulting in execution of scripts with Administrator privileges on system reboot.

CVE-2025-11696 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2025-11696. A base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.2 SERVER-SIDE REQUEST FORGERY (SSRF) CWE-918

A local server-side request forgery (SSRF) security issue exists within Studio 5000 Simulation Interface via the API. This vulnerability allows any Windows user on the system to trigger outbound SMB requests, enabling the capture of NTLM hashes.

CVE-2025-11697 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2025-11697. A base score of 8.8 has been calculated; the CVSS vector string is (AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Chemical, Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United States

3.4 RESEARCHER

Rockwell Automation reported these vulnerabilities to CISA.

4. MITIGATIONS

Rockwell Automation recommends that users upgrade to version 3.0.0 or later.

Users who are unable to upgrade to the corrected version are encouraged to follow Rockwell Automation's security best 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. 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 these vulnerabilities has been reported to CISA at this time. These vulnerabilities are not exploitable remotely.

5. UPDATE HISTORY

November 13, 2025: Initial republication of Rockwell Automation advisory 'Studio 5000 Simulation Interface - Multiple Vulnerabilities'

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-06>