Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Rockwell Industrial Control Systems - 2nd September 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	149
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-02
Issue Date	2026-09-01

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Multiple vulnerabilities have been identified in the following Rockwell Automation ICS products: Historian ME, ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix, FactoryTalk Activation Manager, Logix Platform, Redundancy Module Configuration Tool, and RSLinx Classic. Successful exploitation of the vulnerabilities addressed in these advisories could result in privilege escalation, remote code execution, or denial-of-service conditions on affected systems.

Rockwell Automation Historian ME

Summary

Successful exploitation of these vulnerabilities could crash the device being accessed; an out-of-bounds write condition may allow remote code execution.

The following versions of Rockwell Automation Historian ME are affected:

- **Series B 5.202 (CVE-2025-12768, CVE-2026-12661)**
- **Series C 7.101 (CVE-2025-12768, CVE-2026-12661)**

- **CVSS v3 8**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation Historian ME
- **Vulnerabilities:** Out-of-bounds Write, Stack-based Buffer Overflow

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-12768	High	A security issue exists within FactoryTalk® Historian Machine Edition. An attacker with low-level authentication could exploit this vulnerability to achieve remote code execution on the affected device.
CVE-2026-12661	Medium	A denial-of-service security issue exists within FactoryTalk® Historian Machine Edition. A network adjacent attacker who is authenticated could send crafted requests to the web interface, resulting in buffer overflow conditions that may cause the device to crash and become unresponsive.

Remediation:

- Customers using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automations security best practices found at https://support.rockwellautomation.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight.

Rockwell Automation ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix

Summary

Successful exploitation of this vulnerability could result in a denial of service on the affected device.

The following versions of Rockwell Automation ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix are affected:

- **ControlLogix 5580 <34.015, <35.014, <36.013, <37.011 (CVE-2021-42260, CVE-2021-42260, CVE-2021-42260, CVE-2021-42260)**
- **GuardLogix 5580 <34.015, <35.014, <36.013, <37.011 (CVE-2021-42260, CVE-2021-42260, CVE-2021-42260, CVE-2021-42260)**
- **CompactLogix 5380 <34.015, <35.014, <36.013, <37.011 (CVE-2021-42260, CVE-2021-42260, CVE-2021-42260, CVE-2021-42260)**
- **Compact GuardLogix 5380 <34.015, <35.014, <36.013, <37.011 (CVE-2021-42260, CVE-2021-42260, CVE-2021-42260, CVE-2021-42260)**
- **CompactLogix 5480 <34.015, <35.014, <36.013, <37.011 (CVE-2021-42260, CVE-2021-42260, CVE-2021-42260, CVE-2021-42260)**

- **CVSS v3 7.5**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix
- **Vulnerabilities:** Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2021-42260	High	A potential denial of service vulnerability exists in the affected products and can be triggered via corrupt crafted data. This could result in a major nonrecoverable fault (MNRF). A program download is required to recover safety controllers. For non-safety controllers, a stage 2 reset is required to recover.

Remediation:

- Rockwell Automation recommends users update to firmware version 34.015 and later.
- Rockwell Automation recommends users update to firmware version 35.014 and later.
- Rockwell Automation recommends users update to firmware version 36.013 and later.
- Rockwell Automation recommends users update to firmware version 37.011 and

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

Rockwell Automation FactoryTalk Activation Manager

Summary

Successful exploitation of this vulnerability could allow an authenticated attacker to obtain elevated system privileges.

The following versions of Rockwell Automation FactoryTalk Activation Manager are affected:
- **FactoryTalk Activation Manager V5.02_and_below (CVE-2026-16675)**

- **CVSS v3 7.8**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation FactoryTalk Activation Manager
- **Vulnerabilities:** Improper Restriction of Excessive Authentication Attempts

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-16675	High	A privilege escalation vulnerability exists within FactoryTalk Activation Manager. The vulnerability stems from custom actions in the installer that spawn visible console windows running with SYSTEM privileges during installation or repair operations. An authenticated attacker with Windows credentials could hijack these console windows to obtain a SYSTEM-level command prompt, allowing full access to all files, processes, and system resources.

Remediation:

- Rockwell Automation recommends users update to software version V5.03.
- Customers using the affected software who are not able to upgrade to one of the corrected versions should use Rockwell Automation's security best practices.

Rockwell Automation Logix Platform

Summary

Successful exploitation of this vulnerability could result in a denial of service on the affected device.

The following versions of Rockwell Automation Logix Platform are affected:
- **ControlLogix 5580 <=V33, V34.011-V34.014, V35.011-V35.013, V36.011-V36.012 (CVE-2026-9637, CVE-2026-9637, CVE-2026-9637, CVE-2026-9637)**
- **CompactLogix 5380 <=V33, V34.011-V34.014, V35.011-V35.013, V36.011-V36.012 (CVE-2026-9637, CVE-2026-9637, CVE-2026-9637, CVE-2026-9637)**
- **GuardLogix 5580 <=V33, V34.011-V34.014, V35.011-V35.013, V36.011-V36.012 (CVE-2026-9637, CVE-2026-9637, CVE-2026-9637, CVE-2026-9637)**
- **Compact GuardLogix 5380 <=V33, V34.011-V34.014, V35.011-V35.013,**

V36.011-V36.012 (CVE-2026-9637, CVE-2026-9637, CVE-2026-9637, CVE-2026-9637)

- **CVSS v3 7.5**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation Logix Platform
- **Vulnerabilities:** Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-9637	High	A denial-of-service vulnerability exists in the affected Logix platforms due to improper validation of input length during CIP message processing. This can result in a major nonrecoverable fault (MNRF), requiring a power cycle to recover.

Remediation:

- Rockwell Automation recommends users update to firmware version V37.011.
- Rockwell Automation recommends users update to firmware version 34.015.
- Rockwell Automation recommends users update to firmware version 35.014.
- Rockwell Automation recommends users update to firmware version 36.013.
- Customers using the affected software who are not able to upgrade to one of the corrected versions should use Rockwell Automation's security best practices.

Rockwell Automation Redundancy Module Configuration Tool

Summary

Successful exploitation of these vulnerabilities could allow an attacker to escalate and execute processes with administrator privileges.

The following versions of Rockwell Automation Redundancy Module Configuration Tool are affected:

- **Redundancy Module Configuration Tool 10.00.00 (CVE-2026-9633)**
- **Redundancy Module Configuration Tool >=9.00.00|<=10.00.00 (CVE-2026-9634)**

- **CVSS v3 7.3**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation Redundancy Module Configuration Tool
- **Vulnerabilities:** Incorrect Default Permissions

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-9633	High	A security issue exists within the Redundancy Module Configuration Tool. The RM3ConfigTool.exe binary searches

		directories in the system path for a required DLL, and one or more of these directories may be writable by standard (non-administrator) users due to incorrect default permissions. If a local attacker places a malicious DLL in such a directory and an administrator subsequently runs the tool, the malicious DLL is loaded into the elevated process and executes with Administrator/SYSTEM privileges.
CVE-2026-9634	High	A security issue exists within the Redundancy Module Configuration Tool. The RMConfigTool.exe binary searches directories in the system path for a required DLL, and one or more of these directories may be writable by standard (non-administrator) users due to incorrect default permissions. If a local attacker places a malicious DLL in such a directory and an administrator subsequently runs the tool, the malicious DLL is loaded into the elevated process and executes with Administrator/SYSTEM privileges.

Remediation:

- Rockwell Automation has released Redundancy Module Configuration Tool version 10.01.00 for users to install.

Rockwell Automation RSLinx Classic

Summary

Successful exploitation of these vulnerabilities could allow an attacker to cause a denial-of-service condition on the affected product.

The following versions of Rockwell Automation RSLinx Classic are affected:

- **RSLinx Classic <=4.50 (CVE-2026-9621, CVE-2026-9622, CVE-2026-9624, CVE-2026-9625)**

- **CVSS v3 8.6**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation RSLinx Classic
- **Vulnerabilities:** Integer Overflow or Wraparound, Integer Underflow (Wrap or Wraparound), Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-9621	Critical	A denial-of-service security issue exists within RSLinx Classic. The security issue stems from improper handling of a malformed packet. A crafted CIP packet can cause the RSLinx Classic service to crash, requiring a restart of the service to recover.
CVE-2026-9622	Critical	A denial-of-service security issue exists within RSLinx Classic. A crafted CIP packet targeting the Forward Close service can cause the RSLinx Classic service to crash, requiring a restart of the service to recover.
CVE-2026-9624	High	A denial-of-service security issue exists within RSLinx Classic. A

		crafted CIP packet can cause the RSLinx Classic service to crash due to insufficient data length validation, requiring a restart of the service to recover.
CVE-2026-9625	High	A denial-of-service security issue exists within RSLinx Classic. A crafted CIP packet with an oversized embedded message request can cause the RSLinx Classic service to crash, requiring a restart of the service to recover.

Remediation:

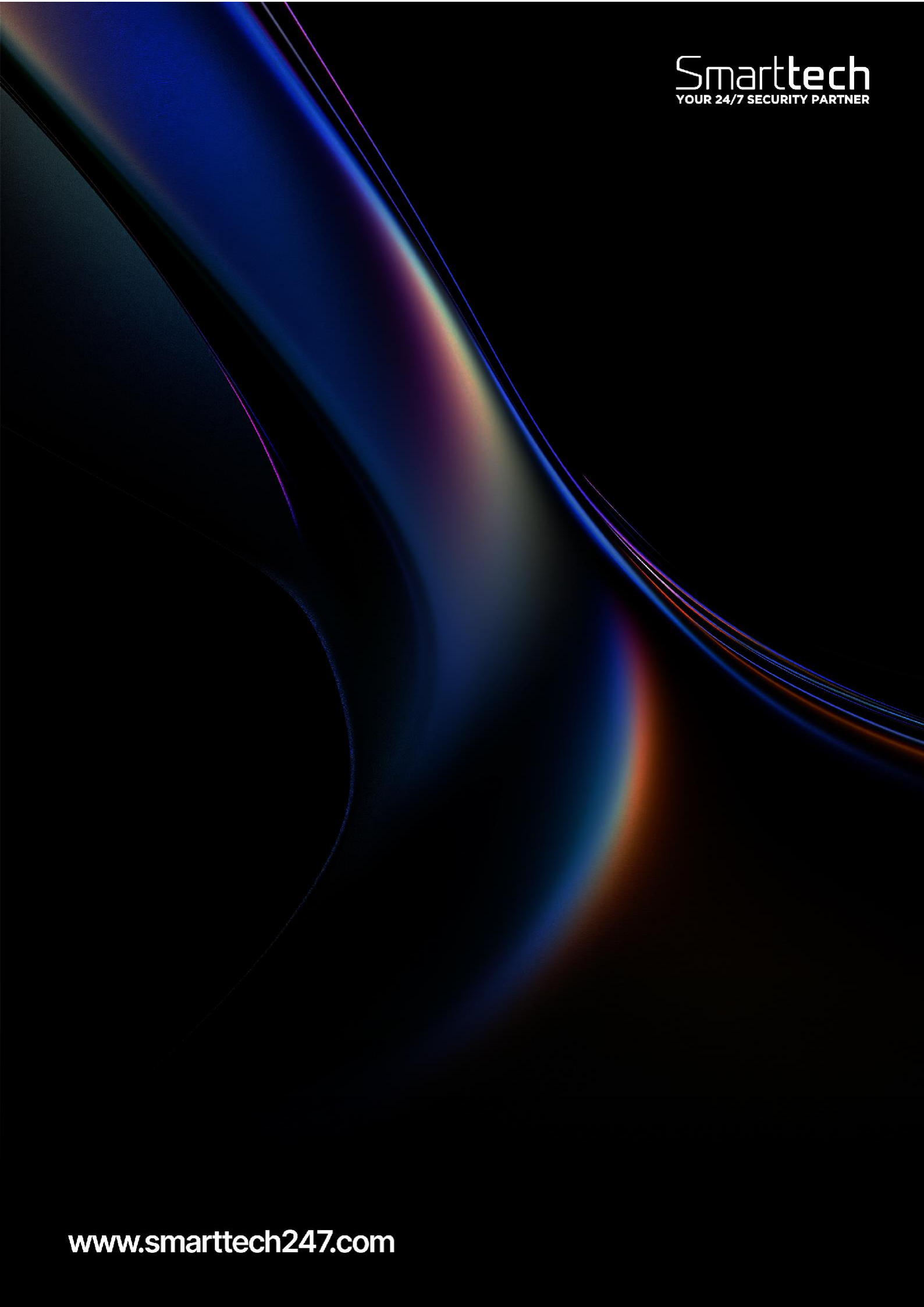
- Rockwell Automation has corrected the vulnerabilities in RSLinx Classic version 4.60.
- Users using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automation's security best practices https://support.rockwellautomation.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight.
- For more information, see Rockwell Automation Security Advisories: https://www.rockwellautomation.com/en-us/trust-center/security-advisories.html.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-244-01

CVEs

CVE-2025-12768
CVE-2026-12661
CVE-2021-42260
CVE-2026-16675
CVE-2026-9637
CVE-2026-9633
CVE-2026-9634
CVE-2026-9621
CVE-2026-9622
CVE-2026-9624
CVE-2026-9625


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com