

CVE-2021-22681

Rockwell Multiple Products Insufficient Protected Credentials Vulnerability

CISA KEV since Mar 5, 2026

Actively exploited

Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480; ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800.

EVRS 80 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.636 99.22nd percentile · FIRST	CISA DEADLINE Mar 26, 2026 CISA federal deadline · Overdue by 7 months
---	---	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.636 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480; ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800.

Affected and fixed versions · 12 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
factorytalk services platform	≥ 2.10	no fixed version listed	NVD
rslogix 5000	≥ 16 ≤ 20	after 20	NVD
studio 5000 logix designer	≥ 21.0	no fixed version listed	NVD
compact guardlogix 5370	—	no fixed version listed	NVD
compact guardlogix 5380	—	no fixed version listed	NVD
compactlogix 1768	—	no fixed version listed	NVD
compactlogix 1769	—	no fixed version listed	NVD
compactlogix 5370	—	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-pvh9-p4pw-h78q	support.rockwellautomation.com	support.rockwellautomation.com/app/answers/answer_view/a_id/1130301/~/%3A-authentication-bypass-vulnerability-found-in-logix-controllers-nvd.nist.gov/vuln/detail/CVE-2021-22681
cisa.gov	cisa.gov/news-events/ics-advisories/icsa-21-056-03	NVD	nvd.nist.gov/vuln/detail/CVE-2021-22681
CISA KEY	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-9817
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-22681		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.