



CVE-2021-22681

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-22681
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-03 18:15:00 UTC
Updated	2022-04-25 16:16:00 UTC
Description	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a k

Risk And Classification

EPSS: 0.129050000 probability, percentile 0.940250000 (date 2026-04-02)

CISA KEV: Listed on 2026-03-05; due 2026-03-26; ransomware use Unknown

Problem Types: CWE-522

CISA Known Exploited Vulnerability

Vendor	Rockwell
Product	Multiple Products
Name	Rockwell Multiple Products Insufficient Protected Credentials Vulnerability
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.
Notes	https://support.rockwellautomation.com/app/answers/answer_view/a_id/1130301/~/~cve-2021-22681%3A-authentication-bypass-vulnerability-found-in-logix-controllers- ; https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03 ; https://nvd.nist.gov/vuln/detail/CVE-2021-22681

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Rockwellautomation	Compactlogix 1768	-	All	All	All
Hardware	Rockwellautomation	Compactlogix 1768	-	All	All	All
Hardware	Rockwellautomation	Compactlogix 1768	-	All	All	All
Hardware	Rockwellautomation	Compactlogix 1769	-	All	All	All
Hardware	Rockwellautomation	Compactlogix 1769	-	All	All	All
Hardware	Rockwellautomation	Compactlogix 1769	-	All	All	All

Hardware	Rockwellautomation	Drivelogix 5/30	-	All	All	All
Application	Rockwellautomation	Factorytalk Services Platform	All	All	All	All
Hardware	Rockwellautomation	Guardlogix 5570	-	All	All	All
Hardware	Rockwellautomation	Guardlogix 5570	-	All	All	All
Hardware	Rockwellautomation	Guardlogix 5570	-	All	All	All
Hardware	Rockwellautomation	Guardlogix 5580	-	All	All	All
Hardware	Rockwellautomation	Guardlogix 5580	-	All	All	All
Hardware	Rockwellautomation	Guardlogix 5580	-	All	All	All
Application	Rockwellautomation	Rslogix 500	All	All	All	All
Application	Rockwellautomation	Rslogix 5000	All	All	All	All
Hardware	Rockwellautomation	Softlogix 5800	-	All	All	All
Hardware	Rockwellautomation	Softlogix 5800	-	All	All	All
Hardware	Rockwellautomation	Softlogix 5800	-	All	All	All
Application	Rockwellautomation	Studio 5000 Logix Designer	All	All	All	All
Application	Rockwellautomation	Studio 5000 Logix Designer	All	All	All	All

References

Reference	Source	Link	Tags
Rockwell Automation Logix Controllers CISA	MISC	us-cert.cisa.gov	Third Party Advisory, US Government Resource
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report