



CVE-2021-22716

Published on: 04/13/2021 12:00:00 AM UTC

Last Modified on: 11/18/2022 11:15:00 PM UTC

CVE-2021-22716

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **C-bus Toolkit** from **Schneider-electric** contain the following vulnerability:

A CWE-732: Incorrect Permission Assignment for Critical Resource vulnerability exists that could allow remote code execution when an unprivileged user modifies a file. Affected Product: C-Bus Toolkit (V1.15.9 and prior)

CVE-2021-22716 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Schneider Electric - C-Bus Toolkit** version < 1.15.9

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	download.schneider-electric.com	MISC download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01

application/pdf

Schneider Electric C-Bus Toolkit | CISA

us-cert.cisa.gov

text/html

MISC us-cert.cisa.gov/ics/advisories/icsa-21-105-01

No Description Provided

download.schneider-electric.com

MISC download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-103-01_C-Bus_Toolkit_C-Gate_Server_Security_Notification.pdf

Inactive Link

Not Archived

ZDI-21-562 | Zero Day Initiative

www.zerodayinitiative.com

text/html

MISC www.zerodayinitiative.com/advisories/ZDI-21-562/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	C-bus Toolkit	All	All	All	All
cpe:2.3:a:schneider-electric:c-bus_toolkit:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →