



CVE-2023-23575

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

Summary

CVE	CVE-2023-23575
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-11 09:15:00 UTC
Updated	2023-04-18 19:36:00 UTC
Description	Improper access control vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker to byp

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Contec	Cps-mc341-a1-111	-	All	All	All
Operating System	Contec	Cps-mc341-a1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-adsc1-111	-	All	All	All
Operating System	Contec	Cps-mc341-adsc1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-adsc1-931	-	All	All	All
Operating System	Contec	Cps-mc341-adsc1-931 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-adsc2-111	-	All	All	All
Operating System	Contec	Cps-mc341-adsc2-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-ds1-111	-	All	All	All
Operating System	Contec	Cps-mc341-ds1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-ds11-111	-	All	All	All
Operating System	Contec	Cps-mc341-ds11-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341-ds2-911	-	All	All	All
Operating System	Contec	Cps-mc341-ds2-911 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341g-adsc1-110	-	All	All	All
Operating System	Contec	Cps-mc341g-adsc1-110 Firmware	All	All	All	All
Hardware	Contec	Cps-mc341q-adsc1-111	-	All	All	All

Operating System	Contec	Cps-mc341q-adsc1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mcs341-ds1-111	-	All	All	All
Operating System	Contec	Cps-mcs341-ds1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mcs341-ds1-131	-	All	All	All
Operating System	Contec	Cps-mcs341-ds1-131 Firmware	All	All	All	All
Hardware	Contec	Cps-mcs341g-ds1-130	-	All	All	All
Operating System	Contec	Cps-mcs341g-ds1-130 Firmware	All	All	All	All
Hardware	Contec	Cps-mcs341g5-ds1-130	-	All	All	All
Operating System	Contec	Cps-mcs341g5-ds1-130 Firmware	All	All	All	All
Hardware	Contec	Cps-mcs341q-ds1-131	-	All	All	All
Operating System	Contec	Cps-mcs341q-ds1-131 Firmware	All	All	All	All
Hardware	Contec	Cps-mg341-adsc1-111	-	All	All	All
Operating System	Contec	Cps-mg341-adsc1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mg341-adsc1-931	-	All	All	All
Operating System	Contec	Cps-mg341-adsc1-931 Firmware	All	All	All	All
Hardware	Contec	Cps-mg341g-adsc1-111	-	All	All	All
Operating System	Contec	Cps-mg341g-adsc1-111 Firmware	All	All	All	All
Hardware	Contec	Cps-mg341g-adsc1-930	-	All	All	All
Operating System	Contec	Cps-mg341g-adsc1-930 Firmware	All	All	All	All
Hardware	Contec	Cps-mg341g5-adsc1-931	-	All	All	All
Operating System	Contec	Cps-mg341g5-adsc1-931 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Download File List CONTEC	MISC	www.contec.com	Product
JVNVU#96198617: Multiple vulnerabilities in Contec CONPROSYS IoT Gateway products	MISC	jvn.jp	Third Party Advi
Download File List CONTEC	MISC	www.contec.com	Product
Download File List CONTEC	MISC	www.contec.com	Product
www.contec.com/api/downloadlogger	MISC	www.contec.com	Mitigation, Vend
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)