



CVE-2023-22331

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

Summary

CVE	CVE-2023-22331
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-20 03:15:00 UTC
Updated	2023-01-26 19:52:00 UTC
Description	Use of default credentials vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthen

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Contec	Conprosys Hmi System	All	All	All	All

References

Reference	Source	Link	Tags
www.contec.com/api/downloadlogger	MISC	www.contec.com	
JVNVU#96873821: Contec CONPROSYS HMI System (CHS) vulnerable to OS command injection	MISC	jvn.jp	
Download License Agreement CONTEC	MISC	www.contec.com	
Contec CONPROSYS HMI System (CHS) Update A CISA	MISC	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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](#)