



CVE-2023-28489

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

Summary

CVE	CVE-2023-28489
State	PUBLIC
Assigner	productcert@siemens.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-11 10:15:00 UTC
Updated	2023-07-11 18:15:00 UTC
Description	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPC185 V05), CP-8050 MASTER MODU

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Cp-8031	-	All	All	All
Operating System	Siemens	Cp-8031 Firmware	All	All	All	All
Hardware	Siemens	Cp-8050	-	All	All	All
Operating System	Siemens	Cp-8050 Firmware	All	All	All	All

References

Reference	Source	Link
Siemens A8000 CP-8050 / CP-8031 Code Execution / Command Injection ≈ Packet Storm	MISC	pack
cert-portal.siemens.com/productcert/pdf/ssa-472454.pdf	MISC	cert-
Full Disclosure: SEC Consult SA-20230703-0 :: Multiple Vulnerabilities including Unauthenticated RCE in Siemens A8000	MISC	secdi
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

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](#)