CVE-2023-28130

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-28130
State	PUBLIC
Assigner	cve@checkpoint.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-26 11:15:00 UTC
Updated	2023-08-02 20:45:00 UTC
Description	Local user may lead to privilege escalation using Gaia Portal hostnames page.

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Gaia Portal	r80.40	-	All	All
Application	Checkpoint	Gaia Portal	r81	-	All	All
Application	Checkpoint	Gaia Portal	r81.10	-	All	All
Application	Checkpoint	Gaia Portal	r81.20	-	All	All

References

Reference	Source	Link
Checkpoint Gaia Portal R81.10 Remote Command Execution ≈ Packet Storm	MISC	packetstormsec
CVE-2023-28130 - Command Injection in Check Point Gaia Portal	MISC	pentests.nl
Full Disclosure: CVE-2023-28130 - Hostname injection leads to Remote Code Execution RCE (Authenticated)	MISC	seclists.org
SecLists.Org Security Mailing List Archive	MISC	seclists.org
support.checkpoint.com/results/sk/sk181311	MISC	support.checkpc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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