CVE-2019-8456

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-8456
State	PUBLIC
Assigner	cve@checkpoint.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-09 21:29:00 UTC
Updated	2020-10-22 17:14:00 UTC
Description	Check Point IKEv2 IPsec VPN up to R80.30, in some less common conditions, may allow an attacker with knowledge of the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Ipsec Vpn	r80.10	All	All	All
Application	Checkpoint	Ipsec Vpn	r80.20	All	All	All
Application	Checkpoint	Ipsec Vpn	r80.10	All	All	All
Application	Checkpoint	Ipsec Vpn	r80.20	All	All	All

References

Reference	Source	Link	Tags
Unauthorized VPN access to internal networks via IKEv2 tunnel (CVE-2019-8456)	MISC	supportcenter.checkpoint.com	Vendor Ad
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.

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