

CVE-2026-50751

Check Point Security Gateway Improper Authentication Vulnerability

Exigent

CISA KEV since Jun 8, 2026

Actively exploited

Ransomware use known

A logic flow weakness in Remote Access and Mobile Access certificate validation in deprecated IKEv1 key exchange allows an unauthenticated remote attacker to bypass user authentication and establish a remote access VPN connection without a valid user password.

EVRS 92/100 Immediate priority	CVSS V3.1 9.3 Critical · NVD	EPSS 0.853 99.72nd percentile · FIRST	CISA DEADLINE Jun 11, 2026 CISA federal deadline · Overdue by 4 months
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.853 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 14 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
gaia os	≥ r80.40 < r81.20 r81.20 r82 r82.10	r81.20	NVD
gaia embedded	≥ r80.20.00 < r81.10.17 r81.10.17 ≥ r80.20.00 < r82.00.10 r82.00.10	r81.10.17 · r82.00.10	NVD
quantum spark 1530	—	no fixed version listed	NVD
quantum spark 1550	—	no fixed version listed	NVD
quantum spark 1570	—	no fixed version listed	NVD
quantum spark 1570r	—	no fixed version listed	NVD
quantum spark 1590	—	no fixed version listed	NVD
quantum spark 1595r	—	no fixed version listed	NVD



Sources

Vendor guidance	support.checkpoint.com/results/sk/sk185033	blog.checkpoint.com	blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/
support.checkpoint.com	support.checkpoint.com/results/sk/sk185033?_gl=1*1wqeqhc*_gcl_au*MTI1MzE5MjI2LjE3ODAwMzQ1NTM	NVD	nvd.nist.gov/vuln/detail/CVE-2026-50751
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-35047
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-50751		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.