CERT-EU

Security Advisory 2026-012

# Critical Vulnerabilities in Check Point Products

*2026-09-10 — v1.0*

**TLP:CLEAR**

*History:*

- *10/09/2026 — v1.0 – Initial publication*

## Summary

On 9 September 2026, Check Point released emergency security updates addressing two critical vulnerabilities affecting **Check Point Security Gateway**, **Security Management Server**, and **Spark Firewall** deployments configured to use Remote Access VPN or Site-to-Site VPN [1,2]. Both vulnerabilities carry a CVSS score of 9.8 and could allow an unauthenticated, remote attacker to execute arbitrary code on affected appliances [1,2].

CERT-EU strongly recommends applying the available hotfixes as soon as possible, prioritising internet-facing and perimeter appliances.

## Technical Details

The vulnerability **CVE-2026-85102**, with a CVSS score of 9.8, is an **improper certificate-data validation vulnerability** in the VPN negotiation flow of Check Point Security Gateway that allows an unauthenticated, remote attacker to execute arbitrary code on the affected appliance [1]. The issue affects deployments using either Site-to-Site VPN or Remote Access VPN [1].

The vulnerability **CVE-2026-85103**, with a CVSS score of 9.8, is a **heap overflow vulnerability** in the VPN certificate ASN.1 decoding flow of Check Point Security Gateway and Security Management Server that allows a remote attacker to execute arbitrary code on the affected appliance [2]. Unlike **CVE-2026-85102**, this vulnerability affects both the Security Gateway and the Security Management Server [2].

## Affected Products

The following Check Point products and versions are affected [1,2]:

- Check Point Security Gateway — R80, R80.10, R80.20, R80.30, R80.40 (End of Support)
- Check Point Security Gateway — R81, R81.10 (End of Support)
- Check Point Security Gateway — R81.10.X
- Check Point Security Gateway — R81.20
- Check Point Security Gateway — R82

- Check Point Security Gateway — R82.00.X
- Check Point Security Gateway — R82.10
- Check Point Security Management Server — all versions listed above
- Check Point Spark Firewall (Centrally Managed and Locally Managed) — all versions listed above

Exploitation of **CVE-2026-85102** requires the deployment to be configured with either Remote Access VPN or Site-to-Site VPN [1]. Exploitation of **CVE-2026-85103** additionally affects the Security Management Server in such configurations [2].

Additional information is available in the vendor's advisories [1,2].

## Recommendations

CERT-EU strongly recommends that all organisations running affected Check Point products apply the available hotfixes immediately [1].

## References

[1] https://support.checkpoint.com/results/sk/sk1000117/

[2] https://support.checkpoint.com/results/sk/sk1000118/