TLP:CLEAR【全分野】

別紙

2026 年 9 月 24 日

内閣官房　国家サイバー統括室
対処調整・官民連携等ユニット

Check Point 製品の深刻な脆弱性(CVE-2026-85102)について(注意喚起)

1. 対象ソフトウェア

- Security Gateway： R81.20, R82, R82.10
  R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (EoS)
- Spark Firewall： R81.10.x, R82.00.x

2. 脆弱性悪用による影響等

対象ソフトウェアには、VPN ネゴシエーション処理における証明書検証の不備があり、認証されていないリモートの攻撃者が認証を回避し、対象システム上で任意のコードを実行する可能性があります。

3. 悪用状況

CVE-2026-85102 は、CISA が提供する KEV カタログに追加されており、実際に悪用されていることが確認されています（参考 URL①）。

4. 対応

開発元が提供する情報に基づき、脆弱性が修正された修正プログラムを適用するとともに、必要に応じて開発元の手順に従い、侵害の有無を確認することを推奨します（参考 URL②、③）。

5. 緩和策

開発元より緩和策が提供されています。Jumbo Hotfix Accumulator または Check Point LivePatch の適用が直ちに困難な場合は、当該緩和策を実施することで本脆弱性の悪用リスクを軽減できます（参考 URL②）。なお、根本的な対策はアップデートの適用であることから、早期のアップデートを強く推奨します。

参考 URL

① CISA Adds Four Known Exploited Vulnerabilities to Catalog (2026/9/22)
https://www.cisa.gov/news-events/alerts/2026/09/22/cisa-adds-four-known-exploited-vulnerabilities-catalog

② CVE-2026-85102 - Authentication Bypass and Remote Code Execution in Remote Access and Site-to-Site VPN
https://support.checkpoint.com/results/sk/sk1000117

③ Security Advisory – Action Required – Active Exploitation of CVE-2026-85102 and a Management Pre-Authentication Vulnerability CVE-2026-93616
https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/