TLP:CLEAR【全分野】

別紙

2025 年 12 月 23 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

WatchGuard 製品の深刻な脆弱性（CVE-2025-14733）について（注意喚起）

1. 対象ソフトウェア

・WatchGuard Firebox アプライアンス上の FirewareOS ソフトウェア

影響を受けるバージョン等

-2025.1.4 より前のバージョン（2025.1 系：2025.1 から 2025.1.3 まで）
-12.11.6 より前のバージョン（12.x 系：12.0 から 12.11.5 まで）
-11.x 系の全バージョン（※11.x 系は EOL となっています）

2. 脆弱性悪用による影響等

対象ソフトウェアにおいて、認証されていないリモートの攻撃者による任意のコード実行につながる恐れがあります。

3. 悪用

開発元において、脅威アクターによる脆弱性を悪用した攻撃が確認されています（参考①）。また、対象製品が国内で広く利用されている事が確認されており、今後被害が拡大する恐れがあります（参考②、③）。

4. 対応

参考①の推奨事項を元に、対象ソフトウェアを最新バージョンへ更新を強く推奨します。修正済みバージョンをすぐに適用できない場合、WatchGuard 社の推奨事項（参考④）に従い、一時的な回避策を適用してください。また、サポートが終了している製品が残存している場合、機器の廃止及び後続製品/代替製品への更新を検討することを推奨します。

参考 URL

① WatchGuard Firebox iked Out of Bounds Write Vulnerability（WatchGuard 社）
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

② WatchGuard 製 Firebox の iked における境界外書き込みの脆弱性（CVE-2025-14733）に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2025/at250027.html

③ WatchGuard Firebox の脆弱性対策について（CVE-2025-14733）（CVE-2025-55182）（IPA）
https://www.ipa.go.jp/security/security-alert/2025/alert20251223.html

④ Secure Access to Branch Office VPNs that Use IPSec and IKEv2（WatchGuard 社）
https://techsearch.watchguard.com/KB?type=Article&SFDCID=kA1VrOOOOOODMXNKA4&lang=en_US