TLP:CLEAR【全分野】

別紙

2026 年 8 月 19 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

Microsoft 製品の深刻な脆弱性(CVE-2026-33824)について(注意喚起)

1. 対象ソフトウェア

・Microsoft Windows 10、11
・Microsoft Windows Server 2016、2019、2022、2025

2. 脆弱性悪用による影響等

本脆弱性を通じて、認証されていない攻撃者が、特別に細工されたパケットをインターネットキー交換(IKE)バージョン 2 が有効な Windows マシンに送信することで、リモートコード実行が可能になる恐れがあります。

3. 悪用状況

CVE-2026-33824 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

Microsoft 社より、2026 年 4 月のセキュリティ更新プログラム（参考 URL②）が公開されており、本脆弱性の修正（参考 URL③）についても当該の更新プログラムに含まれているため、早期の適用を強く推奨します。

5. その他

開発元より、セキュリティ更新プログラムをすぐにインストールできない場合の緩和策として、既知のアドレスからの UDP ポート 500 と 4500 への受信トラフィックのみを許可するよう、ファイアウォールルールを設定すること等が推奨されています。(参考 URL③)

参考 URL
① CISA Adds Four Known Exploited Vulnerabilities to Catalog (2026/8/18)
https://www.cisa.gov/news-events/alerts/2026/08/18/cisa-adds-four-known-exploited-vulnerabilities-catalog
② 2026 年 4 月のセキュリティ更新プログラム (Microsoft 社)
https://msrc.microsoft.com/update-guide/releaseNote/2026-Apr
③ Windows インターネットキー交換(IKE)サーバー拡張機能のリモートでコードが実行される脆弱性
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824