TLP:CLEAR【全分野】

別紙

2026 年 1 月 30 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

Ivanti 製品の深刻な脆弱性(CVE-2026-1281、CVE-2026-1340)について(注意喚起)

1. 対象ソフトウェア
   ・Ivanti Endpoint Manager Mobile (EPMM)
   - 12.5.0.0 およびそれ以前
   - 12.6.0.0 およびそれ以前
   - 12.7.0.0 およびそれ以前
   - 12.5.1.0 およびそれ以前
   - 12.6.1.0 およびそれ以前

2. 脆弱性悪用による影響等
   対象ソフトウェアを使用している機器等において、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等の恐れがあります。

3. 悪用
   顧客環境において脆弱性を悪用した攻撃がいくつか確認されています(参考 URL①)。

4. 対応
   対象ソフトウェアの修正パッチの適用を強く推奨します。
   また、開発元が提供する最新の情報を確認の上、脆弱性を悪用する攻撃を受けた可能性があるか調査することを推奨します（参考 URL②)。

5. その他
   開発元より、修正パッチを適用した後に対象ソフトウェアのバージョンをアップグレードすると、修正パッチを再度適用する必要がある点にご注意ください。なお、次回の定期アップデート（12.8.0.0）以降は恒久的な修正が含まれるため、再適用は不要となります。

参考 URL
①Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 & CVE-2026-1340)
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US
②Analysis Guidance Ivanti Endpoint Manager Mobile (EPMM) CVE-2026-1281 & CVE-2026-1340
https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US