TLP:AMBER【全分野】

別紙

2025 年３月 12 日

内閣官房　内閣サイバーセキュリティセンター
対処・外部連携ユニット

Ivanti 製品の深刻な脆弱性(CVE-2025-0282)について(注意喚起)（第２報）

本年１月９日に注意喚起した Ivanti 製品の深刻な脆弱性(CVE-2025-0282)について、国内の政府機関及び独立行政法人において当該脆弱性を悪用するゼロデイ攻撃の事例を確認したことから、改めて注意喚起を行います。対象ソフトウェアを利用する重要インフラ事業者等におかれては、「4.対応」に記載する対応を実施することを強く推奨します。なお、本第２報は第１報（本年１月９日付け（Ivanti 製品の深刻な脆弱性(CVE-2025-0282)について(注意喚起)）の内容を含みます。

1. 対象ソフトウェア

・Ivanti Connect Secure 22.7R2 から 22.7R2.4

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

開発元により脆弱性を悪用した攻撃が確認されています。また、内閣サイバーセキュリティセンターにおいて、国内の政府機関及び独立行政法人に対する本脆弱性を悪用した攻撃を確認しました。

4. 対応

対象ソフトウェアの最新のバージョンへの更新を強く推奨します。なお、開発元より、最新のバージョンへの更新に際して整合性チェックツール(ICT)によるスキャンを行うことが推奨されています。

5. その他

参考として第１報の内容を次ページに掲載します。

参考 URL

- Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways(CVE-2025-0282, CVE-2025-0283)(Ivanti)
  https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283
- Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2025/at250001.html
- Ivanti Connect Secure の脆弱性を利用して設置されたマルウェア SPAWNCHIMERA(JPCERT/CC)
  https://blogs.jpcert.or.jp/ja/2025/02/spawnchimera.html

TLP:CLEAR【全分野】

2025 年１月９日

内閣官房　内閣サイバーセキュリティセンター
対処・外部連携ユニット

Ivanti 製品の深刻な脆弱性(CVE-2025-0282)について(注意喚起)

1. 対象ソフトウェア
・Ivanti Connect Secure 22.7R2 から 22.7R2.4

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
脆弱性を悪用した攻撃が確認されています。

4. 対応
対象ソフトウェアの最新のバージョンへの更新を強く推奨します。なお、開発元より、最新のバージョンへの更新に際して整合性チェックツール(ICT)によるスキャンを行うことが推奨されています。

5. その他
なし

参考 URL

- Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways(CVE-2025-0282, CVE-2025-0283)(Ivanti)
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283
- Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起(JPCERT/CC)
https://www.jpcert.or.jp/at/2025/at250001.html