PHILIPS

2025 年 11 月

株式会社フィリップス・ジャパン

AVW (V15)および PIC iX (C.x, 4.x)のセキュリティ情報に関するお知らせ

Security Advisory の Microsoft Windows Server Update Service Vulnerability (CVE-2025-59287) (2025 October 27)の公開内容に関しまし て、高い深刻度の脆弱性が報告されているため、翻訳と共に日本国内お客様向けに周知させていただきたい情報をお伝えいたします。

<Microsoft Windows Server Update Service Vulnerability (CVE-2025-59287) (2025 October 27) の翻訳>

公開日: 2025 年 10 月 27 日

更新日: 2025 年 11 月 7 日

フィリップスは現在、Microsoft Windows Server（2012、2016、2019、2022、および 2025）の Windows Server Update Service（WSUS）に影響を与える、最近リリースされた重大なリモートコード実行脆弱性（CVE-2025-59287）に関する開発とアップデートを監視しています。

この脆弱性は現在広く悪用されており、悪意のあるコードをリモートで実行できる可能性があります。

フィリップスは、弊社の製品セキュリティポリシーと手順の一環として、フィリップス製品とソリューションが脆弱性の影響を受ける可能性について継続的に評価を行い、対策の検証を行っています。

フィリップスは、フィリップスが承認する製品仕様内で導入・運用される際の製品の安全性、セキュリティ、完全性、規制遵守の確保に取り組んでいます。そのため、フィリップスのポリシーと規制要件に則り、フィリップス製品に対するすべての設定変更やソフトウェアの適用（オペレーティングシステムのセキュリティ更新やパッチを含む）は、フィリップス製品固有の検証・妥当性確認を行い、承認・周知されたお客様向け手順や現場対応に限定して行われます。

契約対象のお客様は Philips InCenter をご利用いただけます。Philips InCenter へのアクセスを要求し、掲載されている製品固有の情報をご参照いただくことを推奨いたします。契約の有無に関わらず、ご不明点があるお客様は、お使いの製品に関する最新情報について、カスタマーケアセンターまでお問合せください。

フィリップスは、この脆弱性によって影響を受ける可能性のあるフィリップス製品を特定するために、以下の製品リストを提供しています。掲載されていない製品は影響を受けないとお考えください。追加の製品が判明した場合、フィリップスは随時リストを更新いたします。

881001 – Advanced Visualization Workspace(V15)[3]　（注 1）

866389 – PIC iX (C.x, 4.x)[1,3]　（注 2）

867113 – Focal Point[1,2,3]　（注 3）

上記の全製品に対し、フィリップスは最善の緩和策を評価しています。具体的な緩和策は以下のとおりです:

1. サポート対象の Windows Server 2016、2019、2022 に適用されます。
2. この脆弱性は、Windows Server Update Service（WSUS）が有効になっている Focal Point Server のインストール環境にのみ影響します。
3. 情報またはパッチは InCenter で入手可能です。

（注1）　販売名：フィリップス Advanced Visualization Workspace／認証番号：306AFBZX00035000

（注2）　販売名：セントラルモニタ フィリップス患者情報センタ／認証番号：22200BZX00715000

販売名：セントラルモニタ フィリップスインフォメーションセンタ／承認番号：30200BZX00351000

（注3）　Focal Point は日本では販売・導入されておりません。

＜国内のお客様向けの周知＞

日本国内のお客様におきましては、本脆弱性の潜在的なリスクを最小限に抑えるため、CVE-2025-59287 （ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287 ）で周知されている以下のいずれかの緩和策を推奨します：

- サーバーで WSUS Server Role が有効になっている場合は、無効化してください[*1]。
  注： WSUS を無効化すると、クライアントはサーバーからの更新を受け取れなくなる点にご注意ください。
- ホスト側のファイアウォールでポート 8530 および 8531 へのインバウンドトラフィックをブロックしてください（ネットワーク／境界ファイアウォールだけでブロックするのではなく）。これにより WSUS が動作しなくなります。

*1 AVW V15 および PIC iX (C.x, 4.x)は、出荷時に WSUS Server Role は無効化されております。

さらに詳細な情報につきましては、フィリップスのサービス担当者にお問い合わせください。

以上