PHILIPS

2025 年 1 月

株式会社フィリップス・ジャパン

【アップデート】Vue PACS のセキュリティ情報に関するお知らせ

Security Advisory Archives (2024)の Philips VuePACS (2024-July-18) の公開内容に関しまして、当初公開時点では高い深刻度の脆弱性が報告されていたため、日本国内お客様向けにお伝えさせていただいておりましたが、その後のさらなる解析の結果、一部の脆弱性は本製品またはセキュリティに影響を与えないことが判明し、深刻度は低下しました。今回アップデートされた公開内容の翻訳と共に日本国内お客様向けにあらためて周知させていただきたい情報をお伝えいたします。

<Philips VuePACS (2024-July-18)の翻訳>

公開日：2024 年 7 月 18 日

更新日：2024 年 11 月 26 日

潜在的なセキュリティ脆弱性の認識と修正を目的としたフィリップスの脆弱性開示ポリシー に従い、Philips Vue PACS バージョン 12.2.8.410 よりも前のものに存在する脆弱性に関してアドバイザリーを発行しています。

特定の状況下において、フィリップスが特定した潜在的なセキュリティ脆弱性により、攻撃者がデータベースにアクセスでき、システムの可用性やデータの整合性に影響を及ぼしたり、サービス不能状態を発生させたりする可能性があります。

現在までにフィリップスでは、患者への危害、これらの問題の悪用、またはこれらの問題に関連付けることができる臨床使用によるインシデントの報告を受けていません。

Company name
Legal entity only if required by law, Visiting address, Postal address, Country, www.philips.com, Tel number, Fax number, Chamber of Commerce and VAT number if required. Use a maximum of three text lines below the company name. Divide different types of information by commas.

フィリップスは、以下の緩和策を推奨します：

- CVE-2021-28165 については、InCenter で入手可能な D000763414 – Vue_PACS_12_Ports_Protocols_Services_Guide に従って Vue PACS 環境を構成する
- CVE-2023-40704 については、脆弱性を悪用されるリスクが低いため、特に対策は不要であるが、フィリップスにデータベースパスワードの変更を依頼することが可能である

フィリップスはこの脆弱性を、アドバイザリーを発行している米国の Cybersecurity Infrastructure and Security Agency(CISA)を含む適切な政府機関にも報告しています。
CISA website: https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-200-01

<国内お客様向けの周知＞
日本国内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に CISA Web サイトにて周知されている以下の緩和策を推奨します：

- Philips Vue PACS サーバーのネットワークへの露出を最小限に抑え、インターネットからアクセスできないようにする。
- Philips Vue PACS サーバーの配置されている医療情報ネットワークをファイアウォールの背後に配置し、他の業務系ネットワークから分離する。
- Philips Vue PACS サーバーへリモートアクセスを要する場合は仮想プライベートネットワーク（VPN）のようなより安全な手段を使用し、VPN のソフトウェアを利用可能な最新バージョンに更新する。また VPN の安全性は、接続機器の安全性と同程度のみであることを認識する。

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