PHILIPS

2024 年 9 月

株式会社フィリップス・ジャパン

Vue PACS のセキュリティ情報に関するお知らせ

Security Advisories (philips.com)の Philips VuePACS (2024-July-18) 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。

<Philips VuePACS (2024-July-18)の翻訳>

公開日：2024 年 7 月 18 日

更新日：2024 年 7 月 19 日

フィリップスの脆弱性開示ポリシー (潜在的なセキュリティ脆弱性の認識と修正) 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ます。特定の状況下において、本脆弱性が、患者の機密性、システムの整合性、あるいはシステムの可用性に影響を与えたり、危険にさらす可能性があります。現在までにフィリップスでは、患者への危害、脆弱性の悪用、または脆弱性に関連した臨床使用によるインシデントの報告を受けていません。

Philips Vue PACS 12.2.8.400 (2023 年 8 月にリリース) にアップグレードすることでほとんどの脆弱性を修正可能で、また 12.2.8.410 (2023 年 10 月にリリース) にアップグレードすることで CWE-400 に該当する脆弱性を修正することができますが、アップグレードを行うまで、脆弱性の潜在的なリスクを最小限に抑えるために以下（次ページ）の緩和策を推奨します：

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.

- InCenter で入手可能な 8G7607 – Vue PACS ユーザー ガイド Rev G に従って Vue PACS 環境を構成する
- 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

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