PHILIPS

2026 年 7 月

株式会社フィリップス・ジャパン

PIC iX 4.x のセキュリティ情報に関するお知らせ

Security Advisory の Microsoft DHCP Advisory (CVE-2026-44815 & CVE-2026-45602) (2026 June 22)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の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 DHCP Advisory (CVE-2026-44815 & CVE-2026-45602) (2026 June 22)の翻訳>

公開日: 2026 年 6 月 22 日

更新日: 2026 年 6 月 22 日

フィリップスは現在、Microsoft Windows DHCP に影響を与える、最近公開されたアドバイザリー（CVE-2026-44815 および 2026-CVE-45602）に関する動向と更新情報を監視しています。Microsoft はこれら 2 件の脆弱性に対するパッチを提供しています。

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、弊社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、弊社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、弊社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弊社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。

PIC iX 4.x [1]（注 1）

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. お客様所有のオペレーティングシステムと組み合わせて使用するソフトウェアのみの製品です。適用が必要な緩和策の実施は、お客様の責任となります。

（注1） 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

＜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-2026-44815 （ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44815 ）および CVE-2026-45602（https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602）で周知されている以下の緩和策を推奨いたします：

Microsoft 社より提供されフィリップスにて検証済みの以下のパッチを適用する

KB5094123 - Windows 10 IoT Enterprise LTSC 2019 (Version 1809)

KB5094127 - Windows 10 IoT Enterprise LTSC 2021 (Version 21H2)

KB5094123 - Windows Server IoT 2019 Standard Edition (Version 1809)

KB5094128 - Windows Server IoT 2022 Standard Edition (Version 21H2)

パッチ適用作業のご依頼に関しては、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