dexcom

2026 年 11 月

DexCom Japan 合同会社
〒153-0064　東京都目黒区下目黒一丁目 8 番 1 号
アルコタワー 7 階

【Dexcom 製品に関連するセキュリティ情報についてのお知らせ】

謹啓

時下ますますご清栄のこととお慶び申し上げます。
平素より弊社製品に格別のご高配を賜り、厚く御礼申し上げます。
このたび、外部で公表されているセキュリティ上の脆弱性に関し、Dexcom 製品およびプラットフォームへの影響について確認を行いましたので、以下のとおりお知らせいたします。

2026 年 10 月 29 日時点において、下記のセキュリティ上の脆弱性による Dexcom 製品およびプラットフォーム環境への影響は確認されておりません。

1. React2Shell

Dexcom 製品およびプラットフォーム環境への影響：なし

対象となるバージョン

・React Server DOM：19.0.x～19.2.x
・Next.js（App Router）：14.x（canary）、15.x、16.x
・RSC（React Server Components）を含む一部のフレームワーク（Vite、Parcel、RedwoodSDK など）も影響を受ける可能性があります。

Dexcom における確認状況

Dexcom の本番環境では、React Server Components（RSC）および Next.js App Router は使用・参照されておらず、悪用可能な該当環境は確認されていません。
また、追加の監視および WAF（Web Application Firewall）による保護対策を実施しています。

2. PHP2Shell

Dexcom 製品およびプラットフォーム環境への影響：なし

対象となるバージョン

以下の PHP バージョンが対象として公表されています。

・PHP 8.2：8.2.35 より前のバージョン
・PHP 8.3：8.3.36 より前のバージョン
・PHP 8.4：8.4.27 より前のバージョン
・PHP 8.5：8.5.12 より前のバージョン
・該当するセキュリティ修正が適用されていない旧バージョン

Dexcom における確認状況

現時点において、Dexcom 製品への影響は確認されておりません。引き続き自社環境および関連するセキュリティ情報の監視を継続しています。

Dexcom のセキュリティ情報について

Dexcom では、Dexcom 製品、サービス、またはそれらを支える技術に影響する可能性のあるセキュリティ情報について、お客様、パートナーおよびその他の関係者の皆様に適時かつ透明性のある情報を提供するため、Product Security Advisories を公開しています。

詳細については、下記をご参照ください。

Product Security Advisories：https://www.dexcom.com/dexcom-security/product-security-advisories

今後も関連するセキュリティ情報を継続的に確認し、適切な情報提供に努めてまいります。今後とも弊社製品をご愛顧賜りますよう、何卒よろしくお願い申し上げます。

謹白

外国特例承認取得者：Dexcom, Inc.
選任製造販売業者：DexCom Japan 合同会社

MAT-18033