脆弱性公開に関するポリシー

株式会社 dots energy（以下「当社」）は、エネルギー貯蔵装置およびエネルギーの運用・管理システム技術を発展させ、世界の持続可能なエネルギーへの移行を加速することに貢献します。このため、当社は独立したエネルギー資産の運用を支援し、システムの安全性を維持するとともに、機密情報が不正に公開されないよう保護します。セキュリティ研究者の皆様には、Quantum 製品で確認された潜在的な脆弱性を当社に報告いただくようお願いいたします。

本ポリシーは以下を明示します。

・どのシステムおよびアプリケーションが対象に含まれるか
・どのような種類のセキュリティ調査手法が許容されるか
・潜在的なセキュリティ脆弱性を当社に報告する方法
・当社の脆弱性公開に対する考え方および脆弱性を公開する前にどの程度の猶予期間を置くか

dots energy は、脆弱性公開ポリシーに準拠した報告を営業日 5 日以内に受領したことを確認します。受領後、提出物の妥当性を検証し、可能な場合は是正措置を実施し、報告された脆弱性の処理状況を研究者にできるだけ遅滞なく通知するよう努めます。

セキュリティ研究を行う際、研究者が本ポリシーに誠実に従う努力をした場合、Quantum の法的セーフハーバー方針に基づき、その研究は承認されたものと見なされます。当社は研究者と協力して問題を迅速に理解・解決し、研究に関連する行為について法的手段を助長または追求することはありません。

テスト方法

セキュリティ研究者は以下の行為を行ってはなりません。

・以下の「範囲」セクションに明記されたシステム以外のシステムをテストすること
・以下の「脆弱性報告」および「公開」セクションに明記された場合を除き、脆弱性情報を公開すること
・施設またはリソースに対する物理的な試験を行うこと
・ソーシャルエンジニアリングに従事すること
・フィッシングメッセージを含む、Quantum のユーザーに対する望ましくないメールを送信すること
・サービス拒否（DoS）やリソース枯渇攻撃を実行または試みること
・Quantum または第三者のシステムにマルウェアを導入すること

・Quantum システムの動作を低下させる、あるいは EMS/PMS システムを意図的に損傷、中断または無効化し得るテストを行うこと
・Quantum システムと統合される、または Quantum システムに接続されている、あるいは Quantum システムから接続されるサードパーティのアプリケーション、ウェブサイト、サービスをテストすること
・Quantum データの削除、変更、共有、保存または破壊、あるいは Quantum データへのアクセス不能を引き起こすこと
・エクスプロイトを用いてデータを流出させる、コマンドラインアクセスを確立する、Quantum システムに永続的な存在を設定する、あるいは他の Quantum システムへ「Pivot」すること

セキュリティ研究者は次の行為が許容されます。

・潜在的な脆弱性の存在を文書化するために必要な範囲内でのみ、Quantum の非公開データを閲覧または一時的に保存すること

セキュリティ研究者は次の行為を行わなければなりません。

・脆弱性を発見した場合は直ちにテストを中止し、当社に通知すること
・非公開データの露出を発見した場合は直ちにテストを中止し、当社に通知すること
・脆弱性を報告する際には、保存したすべての非公開データを削除すること

範囲

以下のシステムおよびサービスが本ポリシーの対象に含まれます。

Quantum
・PMS 運用制御ウェブサイト
・Modbus 通信の制御機能を使用するサーバー

S-Quantum
・PMS 運用制御ウェブサイト
・Modbus 通信の制御機能を使用するサーバー

上に明示的に列挙されていないすべてのサービスは本ポリシーの対象外です。明確化のため、以下を含むがこれらに限定されません。

・スパムフォルダ
・ソーシャルエンジニアリング手法
・サービス拒否攻撃
・コンテンツ注入（Quantum またはユーザーに重大なリスクを明確に示さない限り対象外）

・サンドボックスドメインでのスクリプト実行
・最新の OS バージョンや過去 2 年以内にリリースされたモバイルデバイスで再現できないモバイルアプリのクラッシュ報告
・Quantum のミッション範囲を超えるセキュリティ問題
・極めて稀なユーザー操作を必要とするバグ
・デバイスへの物理的アクセスを必要とする概念実証
・古いソフトウェア—様々な理由で常に最新のソフトウェアを実行しているわけではありませんが、完全にパッチ適用されたソフトウェアを実行する場合
・古いブラウザに影響する欠陥

脆弱性報告

報告は onm@dots-energy.com 宛てのメールで受け付けます。許容されるメッセージ形式はプレーンテキスト、リッチテキスト、HTML です。脆弱性を提出する際には PGP 公開鍵を使用して提出物を暗号化することを推奨します。

・脆弱性の悪用を実証する概念実証（PoC）コードやログを含む報告を歓迎します。
・報告には、脆弱性を特定・再現するために必要な手順を含む、詳細な技術的説明を記載してください（脆弱性を特定または悪用するために必要なツールに関する説明も含むこと）。
・スクリーンショットなどの画像やその他の文書を報告に添付できます。添付ファイルには説明的な名前を付けると助かります。
・スクリプトやエクスプロイトコードは実行不能なファイル形式で添付することを推奨します。
・zip、7zip、gzip を含む一般的なアーカイブ形式を受け付けます。

研究者は匿名で報告を提出することができ、Quantum のセキュリティチームが連絡すべき手段およびタイミングに関する連絡先情報を提供できます。提出された報告の内容を明確化するため、または追加の技術情報を収集するために研究者へ連絡する場合があります。

Quantum に報告を提出することで、研究者は報告およびすべての添付ファイルが第三者の知的財産権を侵害していないことを確認するものとします。また、研究者は Quantum に対して報告および添付ファイルを使用、複製、派生物の生成および公開する非独占的、ロイヤリティフリー、世界的、永続的なライセンスを付与することに同意するものとします。

公開

Quantum は脆弱性を適時に修正するよう最善を尽くします。エネルギー資産の運用を危険にさらす問題を解決するために誠実に取り組みます。容易に利用可能な是正措置がない状態で脆弱性を公開すると、エネルギー資産のセキュリティリスクが低下するどころか増加する可能性があるため、提出された報告をレビューしている間は研究者の皆様のご理解をお願いいたします。

したがって、報告受領の確認を得た後、発見された脆弱性に関する情報を 120 日間共有しないようお願いします。修正が実装される前に他者に脆弱性を知らせる必要があると考える場合は、事前に Quantum セキュリティチームと協議してください。

影響を受けるベンダーと脆弱性報告書を共有することは許容されます。研究者の名前または連絡先情報は明示的な許可がない限り共有しません。

ご不明な点がございますか？

本ポリシーに関する質問は onm@dots-energy.com までお送りください。Quantum は研究者が本ポリシーのあらゆる要素について説明を求めることを歓迎します。

特定のテスト方法が本ポリシーに準拠するか不明な場合、あるいは本ポリシーで扱われていない場合は、テストを開始する前にお問い合わせください。また、セキュリティ研究者の皆様から本ポリシー改善のためのご提案を歓迎します。

本コンテンツの韓国語版と翻訳版に不一致がある場合は、韓国語版が優先されます。