취약점 공개정책

주식회사 다츠에너지는 에너지저장 장치와 에너지 운영 및 관리 시스템 기술을 발전시켜 세계가 지속 가능한 에너지로의 전환을 가속하는데 기여합니다. 그렇기 때문에 저희는 독립적인 에너지 자산 운영을 지원하여 시스템의 보안을 유지하고 민감한 정보가 무단으로 공개되지 않도록 보호합니다. 보안 연구원들이 Quantum 제품에서 확인된 잠재적 취약점을 보고하도록 저희에게 연락할 것을 권장합니다

이 정책은 다음을 명시합니다.

- 어떤 시스템과 애플리케이션이 범위에 포함되는지
- 어떤 유형의 보안 연구 방법이 포함되는지
- 잠재적인 보안 취약점을 저희에게 보고하는 방법
- 저희의 취약점 공개 철학 및 취약점을 공개하기 전에 얼마나 기다려야 하는지

dots energy는 취약점 공개 정책을 준수하는 보고서를 영업일 기준 5일 이내에 접수했음을 확인합니다. 접수 시 제출물의 유효성을 검사하고 시정 조치를 구현하며(해당하는 경우), 보고된 취약점의 처리 결과를 최소한의 지연으로 연구원에게 알리기 위해 노력할 것입니다.
보안 연구 중 이 정책을 준수하기 위해 선의의 노력을 기울이는 경우 Quantum 의 법적 세이프 하버 정책에 따라 귀하의 연구가 승인된 것으로 간주됩니다. 저희는 귀하와 협력하여 문제를 신속하게 이해하고 해결할 것이며, 귀하의 연구와 관련된 어떠한 조치에 대해서도 법적 조치를 권고하거나 추구하지 않을 것입니다.

테스트 방법

보안 연구원은 다음을 해서는 안 됩니다.

- 아래 범위 섹션에 명시된 시스템 이외의 다른 시스템 테스트
- 아래의 '취약점 보고' 및 '공개' 섹션에 명시된 경우를 제외하고 취약점

정보 공개

- 시설 또는 리소스의 물리적 테스트 참여
- 사회 공학 참여
- '피싱' 메시지를 포함하여 Quantum 사용자에게 원치 않는 이메일 전송
- '서비스 거부' 또는 '리소스 고갈' 공격 실행 또는 시도
- Quantum 또는 제3자 시스템에 악성 소프트웨어 도입
- Quantum 시스템의 작동을 저하시키거나 EMS/PMS 시스템을 의도적으로 손상, 중단 또는 비활성화할 수 있는 테스트 수행
- Quantum 시스템과 통합되거나 Quantum 시스템에 연결되거나 Quantum 시스템에서 연결되는 타사 애플리케이션, 웹사이트 또는 서비스 테스트
- Quantum 데이터 삭제, 변경, 공유, 보존 또는 파괴하거나 Quantum 데이터에 접근할 수 없도록 만들기
- 'Exploit'을 사용하여 데이터를 유출하거나, 명령줄 접근을 설정하거나, Quantum 시스템에 영구적인 존재를 설정하거나, 다른 Quantum 시스템으로 'Pivoit'

보안 연구원은 다음을 수행할 수 있습니다.

- 잠재적 취약점의 존재를 문서화하는 데 필요한 범위 내에서만 Quantum의 비공개 데이터 보기 또는 저장

보안 연구원은 다음을 수행해야 합니다.

- 취약점 발견 시 즉시 테스트를 중단하고 저희에게 알림
- 비공개 데이터 노출 발견 시 즉시 테스트를 중단하고 저희에게 알림
- 취약점을 보고할 때 저장된 모든 비공개 데이터 삭제

범위

다음 시스템 및 서비스가 범위에 포함됩니다.

Quantum

- PMS 운영 제어 웹사이트
- Modbus 통신의 제어 기능을 사용하는 서버

S-Quantum

- PMS 운영 제어 웹사이트
- Modbus 통신의 제어 기능을 사용하는 서버

위에 명시적으로 나열되지 않은 모든 서비스는 이 정책의 범위에서 제외됩니다. 명확성을 위해 다음을 포함하되 이에 국한되지는 않습니다.

- 스팸함
- 사회 공학적 기법
- 서비스 거부 공격
- 콘텐츠 주입은 Quantum 또는 사용자에게 중대한 위험을 명확하게 입증할 수 없는 한 범위에서 제외됩니다.
- 샌드박스 도메인에서 스크립트 실행
- 최신 OS 버전 또는 지난 2년 이내에 출시된 모바일 기기에서 재현할 수 없는 모바일 앱 충돌 보고서
- Quantum 의 미션 범위를 벗어나는 보안 문제
- 극히 드문 사용자 상호 작용이 필요한 버그
- 기기에 대한 물리적 접근이 필요한 개념 증명
- 오래된 소프트웨어 — 다양한 이유로 항상 최신 소프트웨어 버전을 실행하지는 않지만, 완전히 패치된 소프트웨어는 실행합니다.
- 오래된 브라우저에 영향을 미치는 결함

취약점 보고

보고서는 onm@dots-energy.com 이메일을 통해 접수됩니다. 허용되는 메시지 형식은 일반 텍스트, 서식 있는 텍스트, HTML입니다. 취약점을 제출할 때 PGP 공개 키를 사용하여 제출물을 암호화할 것을 권장합니다.

- 취약점 악용을 시연하는 개념 증명 코드/로그가 포함된 보고서를 선호합니다.
- 보고서에는 취약성을 식별하거나 악용하는 데 필요한 도구에 대한 설명을 포함하여 취약성을 재현하는 데 필요한 단계에 대한 자세한 기술적 설명이 포함되어야 합니다.
- 이미지(예: 화면 캡처) 및 기타 문서를 보고서에 첨부할 수 있습니다. 첨부

파일에 설명적인 이름을 지정하면 도움이 됩니다.

- 스크립트나 익스플로잇 코드는 실행 불가능한 파일 유형에 포함하도록 요청합니다.
- zip, 7zip, gzip을 포함한 모든 일반적인 파일 유형 및 아카이브를 처리할 수 있습니다.

연구원은 익명으로 보고서를 제출하거나 Quantum 보안팀이 연락해야 하는 방법과 시기를 포함한 연락처 정보를 제공할 수 있습니다. 제출된 보고서의 내용을 명확히 하거나 기타 기술 정보를 수집하기 위해 연구원에게 연락할 수 있습니다.

Quantum에 보고서를 제출함으로써 귀하는 보고서 및 모든 첨부 파일이 제3자의 지적 재산권을 침해하지 않음을 확인합니다. 또한 귀하는 Quantum에 보고서 및 모든 첨부 파일을 사용, 복제, 파생 저작물 생성 및 게시할 수 있는 비독점적, 로열티 프리, 전 세계적, 영구적 라이선스를 부여합니다.

공개

Quantum은 취약점을 시기 적절하게 수정하기 위해 최선을 다하고 있습니다. 에너지 자산의 운영을 위험에 빠뜨리는 모든 문제를 해결하기 위해 부지런히 노력할 것입니다. 쉽게 이용할 수 있는 시정 조치가 없는 상태에서 취약점을 공개하면 에너지 자산의 보안 위험이 감소하기보다는 증가할 가능성이 높으므로, 제출하신 보고서를 검토하는 동안 모든 연구원들께서 양해해 주시기 바랍니다. 따라서 귀하는 보고서 접수 확인을 받은 후 120일 동안 발견된 취약점에 대한 정보 공유를 삼가해야 합니다. 시정 조치를 구현하기 전에 다른 사람에게 취약점을 알려야 한다고 생각되면 Quamtum 보안팀과 사전에 협의해야 합니다. 영향을 받는 공급업체와 취약점 보고서를 공유할 수 있습니다. 명시적인 허가 없이는 보안 연구원의 이름이나 연락처 데이터를 공유하지 않습니다.

궁금한 점이 있으신가요?

이 정책에 관한 질문은 onm@dots-energy.com으로 보내주십시오. Quantum은

보안 연구원들이 이 정책의 모든 요소에 대한 설명을 위해 당사에 문의하는 것을 권장합니다.
특정 테스트 방법이 이 정책과 일치하지 않거나 이 정책에서 다루지 않는지 확실하지 않은 경우 테스트를 시작하기 전에 문의해 주세요. 또한 보안 연구원들이 이 정책 개선을 위한 제안을 위해 당사에 연락하는 것을 환영합니다.

이 콘텐츠의 한국어 버전과 번역본 간에 불일치가 있을 경우 한국어 버전이 우선합니다.