U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Privacy, Access, Civil Liberties, and Transparency
Washington, DC 20528

2024년 6월 20일

동료에게,

아시다시피, 사이버 보안 인프라 보안국 (CISA)의 화학 보안 평가 도구 (CSAT)는 2024년 1월 23일부터 2024년 1월 26일까지 악의적 사이버 침해의 표적이 되어, 인사 보안 프로그램 제출물들과 화학 테러 취약성 정보 (CVI) 승인 사용자 계정에 대한 무단 접근 가능성이 발생하였습니다.

CISA의 조사 결과, 이 데이터들이 유출되었다는 증거는 발견되지 않았으나, 주의 차원에서 CISA의 화학 시설 반테러 표준 (CFATS) 프로그램에 신원 확인을 위해 개인 식별 정보 (PII)를 제출했거나 CVI 승인 사용자 계정을 보유한 모든 개인에게 이 정보가 부적절하게 접근되었을 가능성이 있음을 알려드립니다. 여러분의 우려와 불만을 이해하며, 이번 침해 시도에 대해 저희가 알고 있는 정보를 제공하고자 합니다.

귀하가 이 통지를 받는 이유는 (1) 접근 제한 구역 및/또는 중요 자산에 접근할 수 있는 화학 시설이 인사 보안 프로그램 하에서 신원확인을 위해 귀하의 PII를 제출한 경우, 또는 (2) 2007년 6월부터 2023년 7월 사이에 귀하 또는 화학 시설이 CVI 승인 사용자 계정 생성을 위해 제한된 PII 및 사업 연락처 정보를 제출한 경우. 또한, 침해에 대한 기술적 세부 사항을 관련된 화학 시설과 공유하였습니다.

잠재적 영향을 받을 수 있는 정보

인사 보안 프로그램. CFATS 인사 보안 프로그램은 CFATS 규제를 받는 시설이 위험 기반 성과 표준 (RBPS) 12(iv) - 인사 보안을 준수할 수 있도록 합니다. (RBPS) 12(iv)[1]는 높은 위험을 가진 화학 시설의 제한 구역 및 중요 자산에 접근하거나 접근하려는 시설 직원과 무단 방문자가 잠재적 테러리스트와의 연관성을 확인하기 위해 신원 확인을 받도록 요구합니다. 이는 테러리스트 감시 데이터베이스[2]를 통한 개인의 확인을 위해 CSAT를 통한 PII 제출, 또는 다른 국토안보부 프로그램 하에서 수행된 신원 확인을 재사용하는 것도 포함됩니다.

인사 보안 프로그램을 통해 제출된 PII에는 개인의 이름, 생년월일, 시민권 또는 성별이 포함되어 있습니다. 미국인이 아닌 경우, 필요에 따라 추가적인 PII가 제공되었으며, 다음을 포함합니다:

[1] 6 C.F.R. 27.230(a)12(iv).
[2]테러리스트 감시 데이터베이스에 대한 자세한 내용은 다음 링크를 방문하십시오: https://www.fbi.gov/investigate/terrorism/tsc

- 별명
- 출생지
- 국적
- 여권 번호
- 교정 번호
- 외국인 등록 번호
- 글로벌 엔트리 ID 번호
- TWIC ID 번호

CSAT 사용자 계정. 일반적으로, CSAT에 정보를 제출하는 시설들은 두 가지 유형의 사용자 계정이 있습니다: Top-Screen 설문조사, 보안 취약성 평가 및 사이트 보안 계획(CVI 승인 사용자 포함)을 제출하거나 개발에 참여하는 CSAT 사용자, 그리고 인사 보안 정보를 제출하는 CSAT 사용자. 두 경우 모두, CSAT 계정 생성을 위해 수집되는 정보는 다음과 같이 동일합니다: 이름, 직함, 업무 주소 및 업무 전화번호.

침해 세부 사항

1월 26일, CISA는 CSAT Ivanti Connect Secure 기기에 영향을 미치는 잠재적인 악의적 활동[3]을 발견했습니다. CISA는 즉시 시스템을 오프라인 상태로 전환하고 애플리케이션을 나머지 네트워크에서 격리한 후, 포렌식 조사를 시작했습니다. 이 조사에는 CISA 최고정보책임자실, 사이버 보안 부서의 위협 사냥 팀 및 국토안보부의 네트워크 운영 센터의 기술 전문가들이 포함되었습니다.

조사 과정에서 악의적 공격자가 Ivanti 기기에 고급 웹쉘을 설치한 것을 확인했습니다. 이러한 유형의 웹쉘은 악성 명령을 실행하거나 기본 시스템에 파일을 쓰는 데 사용될 수 있습니다. 추가 분석 결과, 악의적인 공격자가 이틀 동안 여러번 이 웹쉘을 액세스한 것으로 확인되었습니다.

중요한 점은 조사 결과, CSAT 데이터의 유출이나 Ivanti 기기 외의 접근은 없었다고 결론지었습니다. CSAT 내의 모든 정보는 AES 256 암호화를 사용하여 암호화되었으며, 각 애플리케이션의 정보에는 추가적인 보안 제어 기능이 있어 횡적 접근의 가능성을 줄였습니다. 암호화 키는 위협 공격자가 시스템에 접근하는 유형으로부터 숨겨져 있었습니다.

영향을 받은 개인에 대한 권장 사항

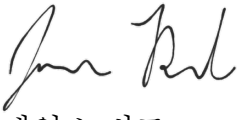
조사 결과 자격 증명 도난의 증거는 발견되지 않았지만, 사이버 공격자의 무차별 대입 공격으로부터 자신을 보호하는 방법에 대한 CISA의 지침(https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), 비밀번호 선택 및

[3]이러한 유형의 악의적 활동에 대한 자세한 내용은 다음 링크를 방문하십시오: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

보호(https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), 그리고 다단계 인증(https://www.cisa.gov/MFA)을 읽고 따를 것을 권장합니다.

CISA는 이 통지서 사본, 자주 묻는 질문, 정기 업데이트 및 이메일 배포 목록에 등록하여 최신 정보를 받을 수 있는 웹사이트를 개설했습니다. CISA에서 추가적으로 가능한 조치를 모색하는 동안, www.cisa.gov/csat-notification 에서 배포 목록에 등록하여 이 사건의 모든 최신 업데이트를 받을 것을 권장합니다. 이번 사건에 영향을 받은 개인의 질문은 CISA 화학 보안 부서(CISA Chemical Security Subdivision)의 CFATS.Notifications@cisa.dhs.gov로 보내주시기 바랍니다.

감사합니다.



제임스 버드
최고 개인정보 보호 책임자