ADT캡스 | infosec

TCO!Stream 취약점

탐지 스크립트 사용 매뉴얼

Top-CERT

2021.04

top-cert@adt.co.kr

[1. 개요]

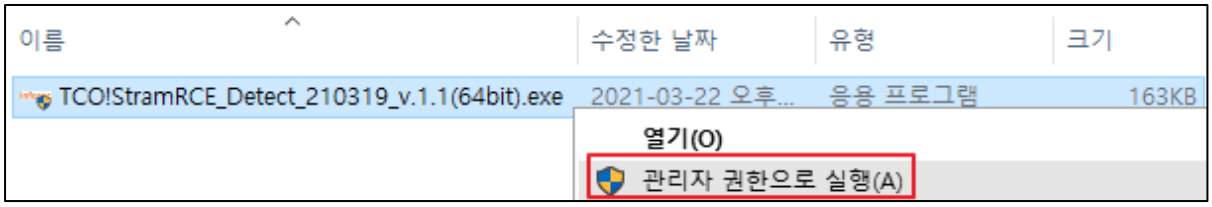
- ㈜엠엘소프트社 자산 관리 솔루션 TCO!Stream 신규 보안 취약점 발견
- 해당 취약점은 에이전트 PC에서 관리 서버로 원격 명령 실행이 가능한 RCE 취약점으로 영향도 '상' 확인
- RCE는 공격자들이 주로 악용하는 취약점이므로 벤더社 문의 후 긴급 패치 적용 권고
  (*) RCE(Remote Code Execution) : 원격에서 임의의 코드 실행이 가능한 취약점으로 영향도 '상'에 해당되며 주로 초기 침투나 내부 거점 확보를 위해 사용
- 에이전트에서 관리 서버로의 원격 명령 실행은 일반적이지 않은 경우로, 결과 파일 내 로그 존재 시 사고 가능성 有
- 2021년 3월 2일 긴급 보안 패치 발표되었으므로 패치 방법 및 패치 파일 벤더社 문의 (version : 8.0.21)
- 해당 RCE 취약점을 식별할 수 있는 침해지표를 식별하여 인지하지 못한 내부 공격 흔적 탐지 / 침해사고 초기 대응 및 원인 규명을 통한 재발방지 방안 마련 효과 기대

[2. 점검 대상]

- TCO!Stream 관리 서버
  (*) TCO!Stream 자산 관리 솔루션 사용 여부 확인 후 관리 서버에서 실행

[3. 사용 방법]

1. 다운로드 받은 첨부 파일 압축 해제 후 TCO!StreamRCE_Detect_210319_v.1.1.exe을 관리자 권한으로 실행



2. TCO!Stream 로그가 저장되어 있는 경로 지정

3. “Seaching TCO!Stream Log...” 문구를 시작으로 로그 검색, 검색 완료 후 “Finished Check Result.txt...” 문구 출력

4. 정상적으로 실행 완료 후 “계속하려면 아무 키나 누르시오...” 문구 출력

[4. 확인 방법]

에이전트에서 관리 서버로의 원격 명령 실행은 일반적이지 않은 경우로, 결과 파일 내 로그 존재 시 정탐

[5. 회신처]

- 소속 ADT 캡스|인포섹 Top-CERT
- E-Mail : top-cert@adt.co.kr

[6. 변경 이력]

- v1.0 : 최초 작성(2021.03)

(끝)