핵심 요약

CrowdStrike 장애 원인분석 및 대책 중간 보고서 (PIR): Falcon 센서 및 Windows 운영 체제에 영향을 미치는 콘텐츠 구성 업데이트 (BSOD)

개요

새롭게 진화하는 사이버 위협에 한발 앞서 대응하기 위해 보안 제품은 정기적으로 콘텐츠 업데이트를 제공합니다. 이러한 업데이트에는 원격 측정 (telemetry) 데이터 수집, 새로운 위협 탐지 패턴, 취약성 탐지 및 기타 중요한 개선 사항이 포함될 수 있습니다. 정기적인 업데이트를 통해 보안 제품은 새로운 위협에 빠르게 적응할 수 있으며, 사용자와 시스템을 강력하게 보호할 수 있습니다.

배경: 장애 발생 경위

2024년 7월 19일 04:09 UTC(한국 시간 13:09)에 센서 버전 7.11 이상을 실행하는 Windows 호스트에 Falcon 센서용 Rapid Response Content업데이트가 배포되었습니다. 이 업데이트는 CrowdStrike가 관찰한 새로운 위협 기술에 대한 원격 측정 (telemetry) 데이터를 수집하기 위한 것이었으나, 04:09 UTC (한국시간 13:09)부터 05:27 UTC (한국시간 14:27) 사이에 온라인 상태였던 시스템에서 충돌(BSOD)을 유발했습니다. Mac과 Linux 호스트는 영향을 받지 않았으며, 해당 기간 동안 온라인 상태가 아니었거나 연결되지 않은 Windows 호스트도 영향을 받지 않았습니다. 이유: 장애 발생 원인.

이유: 장애 발생 원인

이번 충돌은 유효성 검증 과정에서 발견되지 않은 Rapid Response Content의 결함으로 인해 발생했습니다. Falcon 센서가 해당 콘텐츠를 로드할 때 범위를 벗어난(Out-of-Bound) 메모리 읽기가 발생하여 Windows 충돌(BSOD)이 일어났습니다

CrowdStrike의 재발 방지 방안

소프트웨어 테스트 절차 강화

- 다음과 같은 테스트 유형을 사용하여Rapid Response Content 테스트를 강화합니다: 로컬 개발자 테스트, 콘텐츠 업데이트 및 롤백, 스트레스 테스트, 퍼징 (Fuzzing), 오류 주입 (Fault injection), 안정성 및 콘텐츠 인터페이스 테스트.
- Content Validator에 부가적인 유효성 검사를 도입하여 유사한 문제를 방지합니다.

복원력 및 복구 가능성 강화

- 문제 있는 콘텐츠로 인한 오류를 원활하게 처리할 수 있도록 Falcon 센서의 오류 처리 메커니즘을 강화합니다.

배포 전략 개선

- 카나리아 배포 방식으로 소규모 시스템 그룹부터 시작하여 시차를 두고 배포하는 단계적 배포 전략을 채택합니다.
- 시차를 두고 콘텐츠를 배포하는 동안 센서 및 시스템 성능 모니터링을 강화하여 문제를 신속히 식별하고 완화합니다.
- Rapid Response Content업데이트 배포 시기와 위치를 세밀하게 선택할 수 있도록 하여 고객에게 업데이트 제공을 더욱 효과적으로 제어할 수 있도록 합니다.
- 콘텐츠 업데이트 및 시기에 대한 알림을 제공합니다.

제3자 유효성 검사

- 여러 독립적인 제3자 보안 코드 검토를 수행합니다.
- 개발부터 배포까지 엔드 투 엔드 품질 프로세스에 대한 독립적인 검토를 수행합니다.