한국자동차공학회
The Korean Society of Automotive Engineers

자동차 사이버보안연구회
TI 뉴스레터

Published by FESCARO
in collaboration with AUTO-ISAC

- 2026년 4호 -

사보연 TI 뉴스레터 4호에서는 글로벌 모빌리티 사이버보안 규제의 가속화 흐름과, AI 기반 보안 패러다임 변화, 그리고 그 중심에서 확산되고 있는 새로운 위협 양상을 함께 짚어봅니다.

커넥티드 및 자율주행 차량의 확산과 함께, 자동차 산업은 이제 단순한 '제품 보안'을 넘어 **규제 기반의 보안 운영 체계**를 요구받고 있습니다. UN R155의 이륜차 적용 논의부터, 유럽의 Cyber Resilience Act(CRA), 인도의 신규 차량 사이버보안 규정 AIS 189까지, 글로벌 모빌리티 시장 전반에서 '지금 당장 대응해야 하는 규제'가 빠르게 확대되고 있습니다.

동시에 사이버보안의 또 다른 축에서는 거대한 변화가 감지되고 있습니다. AI의 등장에 따라 보안의 중심에 AI가 자리 잡음과 동시에 **새로운 공격 패턴과 취약점의 폭발적 증가**가 지적되고 있습니다. 본 뉴스레터는 최근 등장한 '클로드 미토스(Claude Mythos)'를 둘러싼 논의와 시사점을 다룹니다.

1. 시대의 흐름에 따른 자동차 사이버보안

1) 커넥티드 및 자율주행 차량 시대 자동차 사이버 보안 위협이 증가하고 있습니다.

by DARKREADING

커넥티드 및 자율주행 차량 시대에 자동차 사이버 보안 위협이 증가하고 있습니다.

"완전히 연결된 시스템은 곧 위협을 의미합니다."라고 파딜라는 말했습니다. "이는 위험한 상황입니다. 경각심을 가져야 합니다. 제대로 보안된 차량을 만들기 위해 이 문제를 해결해야 합니다." 현대 자동차는 잠재적인 무기가 될 수도 있습니다. 운전자로부터 차량 제어권을 빼앗기면 치명적인 결과를 초래할 수 있습니다. 최근 몇 년 동안 전 세계 정부는 차량 보안에 대한 우려가 커지고 있으며 이를 규제하기 위한 조치를 취하고 있습니다. 차량이 더욱 정교해지고 연결성이 강화되어 이제는 자율주행 차량까지 등장하면서 이러한 우려는 더욱 커지고 있다고 갈리는 말했습니다.

애널리스트 코멘트 : 이 기사는 RSAC 프레젠테이션의 개괄적인 내용을 제공하며, 현 시대의 자동차 사이버 보안 환경에 대한 전반적인 시각을 제시하지만 다소 과장된 측면도 있습니다.

자세히 보기

2. 글로벌 모빌리티 사이버보안 규제

2) UN R155, 오토바이에 적용: 이륜차 OEM, 지금 당장 갖춰야 할 사항

by CYEQT

오토바이, 모페드, 삼륜차, 사륜차 등 이륜차 제조업체는 이제 승용차 OEM이 2022년부터 적용받아온 UN R155 규정을 동일하게 준수해야 합니다. 주요 요건은 다음과 같습니다.

- 실효성 있는 사이버 보안 관리 시스템(CSMS) 구축 및 운영
- 차량 전체 수명주기를 포괄하는 위험 평가
- 실질적인 운영 능력을 바탕으로 한 공급업체 검증.

애널리스트 코멘트 : 본 기사는 이륜차가 구조적으로는 승용차보다 단순하고 공격 표면 관리가 용이하지만, 분산된 공급망, 소규모 엔지니어링 팀, AUTOSAR 기준이 없는 다양한 ECU 아키텍처, 그리고 각기 다른 규정 체계 하에 운영되는 생산 현장 등으로 인해 상당한 압박을 받을 것으로 예상된다는 점을 강조합니다.

자세히 보기

---

3) 지금이 바로 CRA 시행에 대비할 때입니다

by sonatype

2024년 EU 사이버 복원력법(CRA)이 제정되면서, 기업들이 소프트웨어를 개발, 배포, 유지 관리하는 방식에 중대한 영향을 미치는 세계적인 규제 변화 중 하나가 되었습니다. 이 법은 유럽 연합 내에서 판매되거나 EU에서 사업을 운영하는 기업이 생산하는 하드웨어 및 소프트웨어 제품에 대한 사이버 보안 요건을 규정하며, 사이버 보안 요건에 초점을 맞춘 최초의 국제 법률 중 하나입니다. 또한 소프트웨어 공급망 보안에 대한 관심을 집중시킨 전 세계적인 규제 물결의 일환이기도 합니다. CRA 요건 중 일부는 올해 9월부터 시행되며, 전면 시행은 2027년 12월부터 시작됩니다. 준비할 시간이 충분해 보일 수도 있지만, 눈 깜짝할 사이에 다가올 것입니다. 제품 보안, 엔지니어링, 그리고 규정 준수 팀은 지금보다 더 많은 준비 시간을 가질 수 없으므로, 규제 요건을 실질적인 조치로 전환하는 작업을 이미 시작해야 합니다. 이러한 이유로 저희는 최근 웨비나 "CRA 규제 집행 대비: 소프트웨어 팀을 위한 단계"에서 두 명의 업계 전문가를 초청하여 이 주제에 대해 논의했습니다. Sonatype의 OSPO 기술 프로그램 관리자인 Eddie Knight와 OpenSSF의 최고 기술 책임자이자 Linux Foundation의 최고 보안 설계자인 Christopher Robinson이 팀의 준비 방법에 대한 질문에 답변했습니다. 이들은 위험 평가, 사고 대응, 데이터 보호, 거버넌스, 소프트웨어 공급망 투명성 등 조직이 지금 당장 취할 수 있는 실질적인 조치에 초점을 맞춰 논의했습니다.

애널리스트 코멘트 : 사고 대응 준비 태세는 특히 규제 기관에 대한 신속한 보고 기한과 관련하여 가장 큰 운영상의 격차 중 하나로 지적됩니다. 엔지니어링, 법무, 홍보 및 마케팅 팀이 참여하는 모의 훈련을 통해 실제 사고 발생 전에 대응 계획을 검증하는 것이 좋습니다.

자세히 보기

4) 인도의 AIS 189가 업계에 미치는 영향과 바로 조치를 취해야 하는 이유

by CYEQT

구체적인 일정으로 보면, AIS 189는 다음과 같이 단계적으로 도입됩니다.

- 2024년부터: 제조업체들이 거버넌스 체계를 구축합니다.
- 2025년부터: OEM 업체들이 개발 및 공급업체 관리 시스템에 CSMS(사이버 보안 관리 시스템) 프로세스를 통합합니다.
- 2026~2027년: 사이버 보안 규정 준수가 차량 형식 승인의 일부가 될 것으로 예상되며, 따라서 커넥티드 차량의 경우 사실상 시장 진출 필수 요건이 될 것입니다.

애널리스트 코멘트 : AIS 189는 M 및 N 카테고리 차량과 경량 및 중량 상용차(M2, M3 및 N 카테고리)에 적용되는 것으로 알려져 있습니다. 또한 ECU가 하나 이상 설치된 경우 T 카테고리 차량과 SAE 레벨 3 이상의 자율 주행 기능을 갖춘 L7 차량에도 적용됩니다. 시스템 책임이 있는 OEM, 수입업체 또는 1차 협력업체는 승인 후 AIS 189를 우회할 수 없습니다. UN R155의 현지화 버전에 대한 업계 경험은 형식 승인을 획득하기 위해 국가별 프로세스를 준비해야 함을 시사합니다.

자세히 보기

---

3. AI 사이버위협의 등장

5) RSAC 2026: AI가 주도권을 잡았지만, 커뮤니티는 여전히 보안의 핵심

by DARKREADING

올해 컨퍼런스에서는 AI가 중심 주제로 떠올랐으며, 전문가들은 자동화, 감독, 그리고 사이버 보안에서 인간 지능의 진화하는 역할에 대해 논의했습니다. 미국 정부의 불참이라는 아쉬운 점에도 불구하고 말입니다. RSAC 2026 컨퍼런스는 전 세계 사이버 보안 전문가들이 모여 인공지능(AI)을 중심으로 변화하는 디지털 보안 환경에 대해 논의하는 자리였습니다. 컨퍼런스의 공식 주제인 "커뮤니티의 힘"은 사이버 보안 문제 해결에 있어 인간 협력의 중요성을 강조했지만, AI에 대한 집중적인 논의는 AI의 혁신적인 잠재력과 동시에 AI가 가져올 위험성을 부각시켰습니다. 이번 월간 기자 공동 취재 시리즈 최신 편에서는 Dark Reading의 뉴스 디렉터인 Rob Wright, TechTarget SearchSecurity 수석 사이트 에디터인 Alissa Irei, 그리고 Cybersecurity Dive의 수석 기자인 Eric Geller가 현장 경험을 바탕으로 이번 쇼의 주요 주제들을 논의합니다. 여기에는 보안 운영 센터(SOC)의 획기적인 활용 사례와 AI 기반 취약점에 대한 우려가 포함됩니다.

애널리스트 코멘트 : 컨퍼런스 세션의 3분의 2 이상을 차지하는 주요 주제는 인공지능(AI)이었으며, AI를 신속하게 도입해야 한다는 기업의 압력과 감독 및 거버넌스 부족에 대한 보안 연구원들의 경고 사이에 뚜렷한 긴장감이 존재했습니다.

자세히 보기

---

6) '바이브 코딩'에 대한 안전장치 필요해, AI 보안 우려 고조... NCSC(국가 사이버 보안센터) 경고

by THE CYBER EXPRESS

NCSC(국가 사이버보안센터)의 리처드 호른 CEO는 AI 기반 개발, 흔히 '바이브 코딩'으로 불리는 기술이 분명한 효율성 향상을 제공하지만, 장기적인 사이버보안 영향은 얼마나 책임감 있게 구현되는지에 달려 있다고 강조했습니다. 그는 적절한 안전장치가 없다면 이 기술이 소프트웨어 시스템의 기존 취약점을 더욱 심화시킬 수 있다고 경고했습니다. 호른 CEO는 RSA 컨퍼런스 기조연설에서 디지털 시스템의 고질적인 문제, 즉 악용 가능한 취약점의 만연에 대해 지적했습니다. 그는 이를 "우리가 사용하는 기술의 품질에 대한 근본적인 문제"라고 설명하며, AI가 이러한 결함을 복제하거나 확장해서는 안 된다고 강조했습니다. 호른은 "바이브 코딩의 매력은 분명하다"며, "지속적으로 취약한 수동 소프트웨어의 현상 유지를 깨뜨리는 것은 엄청난 기회이지만, 그 자체로 위험이 따르는 것은 아니다"라고 말했습니다. 그는 또한 AI 도구는 처음부터 신중하게 설계되어야 한다고 덧붙였습니다. "코드를 개발하는 데 사용하는 AI 도구는 의도치 않은 취약점을 도입하거나 확산시키지 않도록 처음부터 설계하고 학습시켜야 합니다." NCSC의 AI 생성 코드에 대한 입장 호른의 RSA 컨퍼런스 연설과 함께, NCSC는 3월 24일 블로그 게시물을 통해 AI 생성 코드가 현재 많은 조직에 "용납할 수 없는 위험"을 초래한다고 경고했습니다. 동시에, 바이브 코딩이 소프트웨어 개발의 "새로운 패러다임의 가능성"을 보여준다는 점도 인정했습니다.

💬 애널리스트 코멘트 : AI 개발 툴을 소프트웨어 파이프라인에 통합하는 OEM 및 공급업체는 생산성 향상 여부와 관계없이 AI 생성 코드가 프로덕션 환경에 도달하기 전에 최소한의 보안 검토 요구 사항을 정의해야 합니다.

자세히 보기

---

4. 신규 공격 기법과 클로드 미토스의 등장

7) SANS: 주목해야 할 가장 위험한 새로운 공격 기법 5가지

by DARKREADING

SANS 연구원들은 매년 RSAC 컨퍼런스에 참석하여 가장 위험한 공격 기법 5가지를 발표합니다. 하지만 2026년에는 뚜렷한 변화가 있습니다. 바로 모든 공격 기법이 인공지능(AI)을 기반으로 한다는 점입니다. SANS 회장이자 발표 사회자인 에드 스코디스는 5가지 주요 공격 기법을 다룬 기조 강연에서 "AI가 관련되지 않은 공격 추세를 지적한다면 거짓말일 것입니다."라고 설명했습니다. "이것이 바로 업계의 현재 상황입니다." 과거에는 자금력이 풍부하고 정교한 연구진을 보유한 국가 차원의 사이버 보안 기관만이 제로데이 공격을 수행할 수 있었습니다. 하지만 SANS 연구소의 교수진이자 수석 기술 책임자인 조슈아 라이트에 따르면, AI 덕분에 제로데이 공격에 대한 진입 장벽이 무너졌습니다. 실제로, 라이트는 독립 연구원들이 널리 배포된 상용 소프트웨어에서 AI 제로데이 취약점을 발견했으며, 공격자는 단 116달러의 AI 토큰 비용만으로도 이를 악용할 수 있다고 지적합니다. 이는 이전에는 정교한 공격자들이 이러한 제로데이 취약점을 찾는데 수백만 달러를 투자했던 것과 비교하면 상당한 비용 절감입니다.

애널리스트 코멘트 : SANS 연구소의 연례 주요 공격 기법 발표에서 처음으로 확인된 5가지 기법 모두 인공지능(AI)과 관련되어 있습니다. 이는 인공지능이 공격자의 진입 장벽을 낮추는 방법을 보여주는 사례입니다.

자세히 보기

---

8) CSA: CISO, 클로드 미토스 등장 이후의 취약점 폭풍에 대비해야 한다

by DARKREADING

클라우드 보안 연합(CSA)의 새로운 보고서에서 전문가들은 앤트로픽(Anthropic)의 클로드 미토스(Claude Mythos) 출시로 촉발될 수 있는 "AI 취약점 폭풍"에 대해 경고합니다. 앤트로픽의 클로드 미토스 모델이 취약점 관리 생태계를 뒤흔들 위협이 되는 가운데, 보안 전문가들은 최고 정보 보안 책임자(CISO)들이 지금부터 대비를 시작해야 한다고 경고합니다. 이달 초, 앤트로픽은 범용성을 갖춘 대규모 언어 모델(LLM)의 새로운 버전인 클로드 미토스 프리뷰(Claude Mythos Preview)를 공개했습니다. 앤트로픽은 이 모델이 특히 보안 작업에 뛰어난 능력을 발휘한다고 강조했습니다. 앤트로픽에 따르면, 미토스는 주요 운영 체제와 웹 브라우저 전반에 걸쳐 복잡하고 심각도가 높은 취약점을 발견하고 악용할 수 있습니다. 앤트로픽은 최근 실험을 통해 수천 개의 버그를 발견했으며, 여기에는 27년 전에 패치된 오픈BSD의 취약점을 악용하는 방법도 포함된다고 밝혔습니다.

애널리스트 코멘트 : 보안 전문가들은 앤트로픽의 클로드 미토스(Claude Mythos) 모델이 주요 운영 체제와 웹 브라우저 전반에 걸쳐 복잡한 취약점을 발견하고 악용할 수 있으며, 이는 공격자에게 방어자가 패치하기 전에 보안 결함을 찾아낼 수 있는 강력한 새로운 도구를 제공할 수 있다고 경고합니다.

자세히 보기

---

5. AI 속도에 맞서는 법 - 인간의 통찰력에 기반한 능동적인 접근

9) AI 시대는 새로운 유형의 CISO를 요구합니다

by CYBERSCOOP

많은 보안 책임자들이 여전히 과거 시대에 맞춰 구축된 프레임워크를 사용하고 있습니다. 수년 동안 성공은 감사 통과, 취약점 해결, 규정 준수 유지와 같은 고정된 지표로 측정되었습니다. 이러한 지표들은 여전히 가치가 있지만, 예측 가능하고 선형적인 방식으로 변화하는 위협 환경에 맞춰 설계되었습니다. 그러나 오늘날 위협 환경은 실시간으로 변화하고 있습니다. AI는 공격자가 취약점을 식별하고 악용하는 방식을 가속화하고 있으며, 클라우드 환경과 자율 시스템은 끊임없이 변화하는 환경을 조성하고 있습니다. 그 결과, 위험을 측정하는 방식과 실제 위협이 발생하는 방식 사이에 격차가 생기고, 정적인 신호로는 역동적인 위협을 따라잡을 수 없게 되었습니다. CISO는 두 방향에서 압박을 받고 있습니다. 위험은 증가하고 있지만, 이를 측정하기 위한 도구는 그 속도를 따라가지 못하고 있습니다. 기존 지표는 종종 과거의 위협 환경을 반영하기 때문에 보안 책임자는 현재 상황을 제대로 파악하지 못하고 있습니다.

애널리스트 코멘트 : 이 기사는 AI 기반 취약점 발견 및 악용, 특히 Anthropic의 Claude Mythos Preview를 언급하며 이러한 현상이 대부분의 조직이 현재 운영하고 있는 보안 측정 프레임워크를 근본적으로 무너뜨렸다고 지적합니다. 감사 통과, 해결된 취약점 수, 규정 준수 확인과 같은 정적인 지표는 지속적으로 변화하는 위험 상태가 아닌 특정 시점의 상황만을 반영하며, 실제 위험이 전개되는 방식과 보안 팀이 이를 추적하는 방식 사이의 격차는 공격 속도가 빨라짐에 따라 더욱 커지고 있습니다.

자세히 보기

---

10) NIST의 CVE 처리 축소가 사이버 보안 팀에 미치는 영향

by DARKREADING

냉방이 시원하게 가동되는 스코츠데일의 연회장은 거의 미동도 없이 NIST(미국 국립표준기술연구소)의 국가 취약점 데이터베이스(NVD) 프로그램 관리자인 해롤드 부스가 주요 운영 변경 사항에 대해 설명하는 동안 조용했습니다. 그는 NIST가 운영 규모를 축소하고 모든 CVE를 처리하는 대신, 중요도가 높은 CVE에 대한 우선순위를 정하여 데이터베이스를 강화할 것이라고 밝혔습니다. 이는 NVD의 규모가 NIST의 관리 역량을 넘어섰다는 것을 인정하는 것이었으며, VulnCon26 참석자 중 누구도 놀라지 않았습니다. 이 특정 내부 관계자 및 업계 베테랑 그룹은 NIST가 점점 늘어나는 CVE 백로그를 처리하는 데 얼마나 어려움을 겪고 있는지를 따라잡는 것이 얼마나 어려운지 잘 알고 있으며, 특히 2024년에 NIST가 연방 자금의 12%를 삭감당한 이후 인재 확보를 위한 도움이 필요하게 되었습니다. 지난해 NIST의 사이버보안 분야 최고 인력들이 대거 이탈한 것처럼, 전국의 사이버보안 전문가들은 NIST와 CVE 프로그램의 부진을 주시하며 서비스 축소에 대비해 왔습니다.

💬 애널리스트 코멘트 : VulnCon26 참석자들은 NIST의 NVD 프로그램 관리자로부터 CVE 정보 보강을 우선시하기로 한 결정이 근본적인 역량 부족 문제를 반영한다는 설명을 직접 들었습니다. CVE 기록은 2025년 약 4만 건에서 2026년 말 6만 건으로 증가할 것으로 예상되지만, 이를 담당할 직원은 21명으로 변동이 없습니다. 컨퍼런스에 참석한 실무자들은 NIST의 2024년 연방 예산 12% 삭감과 그에 따른 인력 손실 이후 이러한 결과가 널리 예상되었다는 데 의견을 같이 했습니다.

자세히 보기

📌사보연 TI 뉴스레터 4호는 아래 구성원들의 기여를 바탕으로 제작되었습니다.

전문가 의견

- 전상훈 교수 (국민대학교)
- 이해승 상무 (피아이코드)
- 엄선현 부장 (페스카로)
- 남현경 연구원 (현대모비스)

추진 및 편집

- 김호진 상무 (오토노머스A2Z)
- 박상범 책임연구원 (현대모비스)
- 우사무엘 교수 (단국대학교)
- 이태관 책임매니저 (현대자동차)
- 황이슬 과장 (페스카로)

사보연 위협인텔리전스 데이터베이스 → CSMS Audit 대응에 활용하십시오.