1. 보안동향

사이버안보연구소, 주요 회원사들과 함께 KADEX 2024 참가

[미리보기]

정경두 대표 “KADEX 참가 통해 연구소 회원사간 협력 긴밀히 할 것”[보안뉴스 권준 기자] 대한민국국제방위산업전(KADEX: Korea Army International Defence Industry Exhibition)은 K-방산을 대표하는 다양한 무기체계부터 전투력을 지원하는 전력지원체계(비무기체계)까지 대한민국 국방산업 전반의 품목을 통합해 전시하

바로가기

[부고] 한국영상정보연구조합 노영식 전 상근부이사장 부친상

[미리보기]

△내용 : 한국영상정보연구조합 노영식 전 상근부이사장 부친상△고인 : 故 노우석님△발인 : 2024 년 10 월 5 일(토)△빈소 : 서안동농협장례식장 203 호(경상북도 안동시 풍산읍 본마을길 36-22)[권준 기자(editor@boannews.com)]<저작권자: 보안뉴스(www.boannews.com) 무단전재-재배포금지>

바로가기

강원도교육청, 교육감과 함께하는 개인정보보호주간 캠페인 실시

[미리보기]

개인정보보호 캠페인으로 교육 현장 안전하게 보호[보안뉴스 박미영 기자] 강원도교육청은 9 월 30 일부터 10 월 4 일까지 개인정보보호 문화 확산과 인식 제고를 위해 '2024 년 교육감과 함께하는 개인정보보호주간 캠페인'을 실시한다.개인정보보호법 시행일(2011.9.30.)을 맞아 운영되는 개인정보보호주간에는 일상생활과 업무 환경 속에서 개인정보보호의 중요성을

바로가기

인천중구시설관리공단, 보안 강화 위한 '기관 합동 개인정보보호주간 캠페인' 실시

[미리보기]

일상생활 속 개인정보 보호 위한 9 가지 실천 수칙 배부[보안뉴스 박미영 기자] 인천중구시설관리공단이 개인정보보호의 날(9.30.)을 맞아 인천역 광장에서 미추홀구시설관리공단과 합동으로 개인정보보호주간 캠페인을 실시했다고 전했다.개인정보보호주간은 중앙행정기관, 지방자치단체, 소속·산하기관 등이 참여해 개인정보보호 활동을 집중적으로 실시하는 기간을 뜻한다.양

바로가기

국가철도공단, 철도 분야 '사이버위협 시나리오 공모전' 수상작 발표

[미리보기]

철도 분야 사이버위협 시나리오 바탕으로 선제적 예방 및 대응체계 구축[보안뉴스 박미영 기자] 국가철도공단은 국민의 안전과 직결되는 철도시스템의 사이버위협에 대비하기 위해 충청권 대학(원)생을 대상으로 진행한 '2024 사이버위협 시나리오 공모전'의 최종 수상작(국가철도공단 이사장상)을 선정했다고 밝혔다.'2024 사이버위협 시나리오 공모전'은 충청지역 정보

바로가기

---

2. 보안권고문

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-10-02)

[미리보기]

2024-10-23 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Ivanti Endpoint Manager (EPM) contains a SQL injection vulnerability in Core server that allows an unauthenticated attacker within the same network to execute arbitrary code. 2024-10-02 Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability Ivanti CVE-2024-29824

바로가기

NVIDIA 제품 보안 업데이트 권고

[미리보기]

NVIDIA 제품 보안 업데이트 권고 2024.10.02 ㅁ 개요 o NVIDIA 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o NVIDIA 의 NVIDIA Container Toolkit 에서 발생하는 TOCTOU(Time-of-check Time-of-use) Race Condition 취약점(CVE-2024-0132) [1][2] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-0132 NVIDIA Container Toolkit v1.16.1 이하 v1.16.2 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1] ㅁ 참고사이트 [1] https://nvidia.custhelp.com/app/answers/detail/a_id/5582 [2] https://nvd.nist.gov/vuln/detail/CVE-2024-0132 ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 NVIDIA Container Toolkit

바로가기

HPE 제품 보안 업데이트 권고

[미리보기]

HPE 제품 보안 업데이트 권고 2024.10.02 ㅁ 개요 o Hewlett Packard Enterprise 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o HPE Aruba Networking 의 AOS 를 실행하는 Aruba Access Points 에서 발생하는 Command Injection 취약점(CVE-2024-42505) [1][2] o HPE Aruba Networking 의 AOS 를 실행하는 Aruba Access Points 에서 발생하는 Command Injection 취약점(CVE-2024-42506) [1][3] o HPE Aruba Networking 의 AOS 를 실행하는 Aruba Access Points 에서 발생하는 Command Injection 취약점(CVE-2024-42507) [1][4] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-42505 CVE-2024-42506 CVE-2024-42507 AOS-10 AOS-10.6 이상 ~ 10.6.0.2 이하 10.6.0.3 이상 또는 10.7 이상 AOS-10.4 이상 ~ 10.4.1.3 이하 10.4.1.4 이상 또는 10.6.0.3 이상 또는 10.7 이상 Instant AOS-8 Instant AOS-8.12 이상 ~ 8.12.0.1 및 이하 8.12.0.2 이상 Instant AOS-8.10 이상 ~ 8.10.0.13 및 이하 8.10.0.14 이상 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1] ㅁ 참고사이트 [1] https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US[2] [2]https://nvd.nist.gov/vuln/detail/CVE-2024-42505 [3] https://nvd.nist.gov/vuln/detail/CVE-2024-42506 [4] https://nvd.nist.gov/vuln/detail/CVE-2024-42507 ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성:위협분석단

취약점분석팀 키워드 AOS-10 , Instant AOS-8 , HPE Aruba Networking

바로가기

Eyeon Security
information security company

주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2 층(06595)
전화 | 02-2105-4400 (영업문의-1 번, 보안관제문의-2 번, 기술문의-3 번) 팩스 | 02-2105-4456
영업문의 | sales@eosec.co.kr 보안관제 및 기술 문의 | tech@eosec.co.kr