1. 보안동향

씨게이트, AI 가 클라우드 스토리지의 성장동력

[미리보기]

AI 의 데이터 생성량 스토리지 수요 견인클라우드 스토리지 시장, 3 년간 두 배 이상 커져[보안뉴스 조재호 기자] 인공지능(AI)이 전례 없는 양의 데이터를 생성해 클라우드 스토리지 수요가 급증할 것이라는 전망이 나왔다.데이터 스토리지 기업 씨게이트 테크놀로지(이하 씨게이트)가 시장조사 기관 리콘 애널리틱스에 의뢰해 한국을 포함한 10 개국 15 개 산업군을 대

바로가기

과기정통부, '연구보안' 주제로 출연연과 현장 소통

[미리보기]

출연연 연구보안 감담회, 국가 R&D 연구보안 정책 추진방향 공유[보안뉴스 김영명 기자] 대한민국 연구보안 기관장들이 한자리에 모였다.16 일 류광준 과학기술정보통신부 과학기술혁신본부장은 '제 28 차 R&D 미소공감' 일환으로 대전 한국전자통신연구소에서 '연구보안'을 주제로 주요 출연연 기관장들과 간담회를 개최하였다. R&D 미소공감은 'R&D 현장과 미래를

바로가기

AI 기본법 거버넌스, '신뢰성' 기반한 기술 생태계 발전

[미리보기]

3 줄 요약 1. 국회의원회관서 AI 기본법 거버넌스 논의 2. "민관 협력해 신뢰 기반 AI 생태계 기대해"3. AI 주도권, 기술 우위 보다 활용·관리 능력[보안뉴스 조재호 기자] 산학연 전문가와 관계부처 그리고 법률 및 기술 자문까지 한목소리로 인공지능(AI) 강국을 위해 '신뢰' 기반의 생태계 조성을 말했다. AI 의 근간인 데이터 관리와 안전한 활용을 강

바로가기

MS, 시큐리티 코파일럿으로 보안시장 저변 확대

[미리보기]

3 줄 요약 1. 시큐리티 코파일럿, 엔드 포인트 보안시장 강자 자리매김 2. 도입 3 개월 만에 보안사고 해결 시간 30% 단축 3. 신뢰 가능 AI 추구, 보안·안전·프라이버시 강화 노력[보안뉴스 조재호 기자] 마이크로소프트(MS)가 인공지능(AI) 시대 보안 전략으로 통합 플랫폼을 제시했다. 자사의 생성형 AI 모델인 시큐리티 코파일럿을 활용해 ID, 디바이스

바로가기

KITRI-서울미디어大, 보안인재 양성 맞손

[미리보기]

사이버보안 인력양성 위한 협력체계 구축교육프로그램 개발, 전문인력 활용 컨설팅 등[보안뉴스 박은주 기자] 한국정보기술연구원과 서울미디어대학원대학교가 힘을 모아 사이버보안 인력 양성에 나선다.한국정보기술연구원(KITRI·원장 유준상)은 서울미디어대학원대학교(SMIT·총장 한희)와 사이버 보안 인력 양성 협력 업무협약을 체결했다고 15 일 밝혔다. 두 기관은 △

바로가기

---

2. 보안권고문

GitHub 제품 보안 업데이트 권고

[미리보기]

GitHub 제품 보안 업데이트 권고 2025.01.16 ㅁ 개요 o GitHub 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o Git for Windows 에서 발생하는 ANSI 이스케이프 시퀀스를 악용한 원격 메시지 조작 취약점(CVE-2024-52005) [1][2] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-52005 Git for Windows 2.48.1 이하 2.47.1 이하 2.46.3 이하 2.45.3 이하 2.44.3 이하 2.43.6 이하 2.42.4 이하 2.41.3 이하 2.40.4 이하 2.47.1(2) ※ 하단의 참고사이트를 확인하여 업데이트 수행 [3] ㅁ 참고사이트 [1] https://github.com/git/git/security/advisories/GHSA-7jjc-gg6m-3329 [2] https://nvd.nist.gov/vuln/detail/CVE-2024-52005 [3] https://lore.kernel.org/git/1M9FnZ-1taoNo1wwh-00ESSd@mail.gmx.net/ ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 Git for Windows

바로가기

SAP 제품 보안 업데이트 권고

[미리보기]

SAP 제품 보안 업데이트 권고 2025.01.16 ㅁ 개요 o SAP 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1][2][3][4][5] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o SAP BusinessObjects Business Intelligence Platform 에서 발생하는 세션 하이재킹 가능한 정보 공개 취약점(CVE-2025-0061) [6] o SAP NetWeaver ABAP 및 ABAP Platform 용 SAP NetWeaver AS 에서 발생하는 SQL Injection 취약점(CVE-2025-0063) [7] o SAP NetWeaver AS for ABAP 및 ABAP Platform(인터넷 통신 프레임워크)에서 발생하는 정보 공개 취약점(CVE-2025-0066) [8] o SAP NetWeaver ABAP Server 및 ABAP Platform 에서 발생하는 부적절한 인증 취약점(CVE-2025-0070) [9] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2025-0061 SAP BusinessObjects Business Intelligence Platform ENTERPRISE 420, 430, 2025 별도 보안 패치 제공 [2] CVE-2025-0063 SAP NetWeaver AS (ABAP 및 ABAP Platform 용) SAP_BASIS 700 이상 ~ 702 이하, 731, 740, 750 이상 ~ 758 이하 별도 보안 패치 제공 [3] CVE-2025-0066 SAP NetWeaver AS (ABAP 및 ABAP Platform[Internet Communication Framework] 용) SAP_BASIS 700 이상 ~ 702 이하, 731, 740, 750 이상 ~ 758 이하, 912 이상 ~ 914 이하 별도 보안 패치 제공 [4] CVE-2025-0070 SAP NetWeaver ABAP Server 및 ABAP Platform KRNL64NUC 7.22, 7.22EXT KRNL64UC 7.22, 7.22EXT, 7.53, 8.04 KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 7.97, 9.12, 9.13, 9.14 별도 보안 패치 제공 [5] ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1][2][3][4][5] ㅁ참고사이트 [1] https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html [2] https://me.sap.com/notes/3474398 [3] https://me.sap.com/notes/3550816 [4] https://me.sap.com/notes/3550708 [5] https://me.sap.com/notes/3537476 [6] https://nvd.nist.gov/vuln/detail/CVE-2025-0061 [7] https://nvd.nist.gov/vuln/detail/CVE-2025-0063 [8] https://nvd.nist.gov/vuln/detail/CVE-2025-0066 [9] https://nvd.nist.gov/vuln/detail/CVE-2025-0070 ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 SAP , BusinessObjects Business Intelligence Platform , NetWeaver ABAP

바로가기

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