1. 보안동향

인기 높은 오픈소스 인공지능 프레임워크 올라마에서 취약점 6 개 발견돼

[미리보기]

개인과 중소기업들이 대형 언어 모델을 구축할 수 있게 해 주는 오픈소스 프레임워크에서 취약점이 발견됐다. 총 6 개로, 4 개는 패치가 됐는데 2 개는 아직이다. 이는 해당 프레임워크의 관리자들이 2 개를 취약점으로 인정하지 않고 있기 때문이다.[보안뉴스 문가용 기자] 오픈소스 인공지능 프레임워크인 올라마(Ollama)에서 6 개의 취약점이 발견됐다. 보안 업체 올

바로가기

심각해지고 있는 아동 대상 온라인 그루밍, 계속해서 늘어나고 있어

[미리보기]

영국에서는 아동을 대상으로 하고 있는 그루밍 범죄가 89% 증가했다고 한다. 이에 좀 더 엄중한 대처와 처벌이 요구되고 있다. 그와 관련하여 보고서가 나왔는데, 여기에는 영국이 아닌 나라에서도 참고할 만한 내용이 담겨 있다.[보안뉴스 문정후 기자] 아동들을 대상으로 한 그루밍 범죄가 6 년 동안 89% 증가했다는 내용의 보고서가 영국에서 나왔다. 흥미로운 건

바로가기

깃 환경 노리는 대규모 캠페인 에머랄드웨일, 클라우드 크리덴셜이 위험하다

[미리보기]

최근 몇 년 동안 크리덴셜은 공격자들이 가장 많이 노리는 자원 중 하나로 자리를 잡았다. 그런데도 크리덴셜 관리가 얼마나 부실한지, 그들은 그리 큰 노력을 하지 않고도 자기들이 원하는 걸 가져가는 편이다. [보안뉴스 문정후 기자] 최근 깃(Git) 환경을 노리는 대형 캠페인이 발견됐다. 에머랄드웨일(EmeraldWhale)이라는 이름이 붙은 이 작전은 보안

바로가기

AI 분야 주요 보안위협 TOP 10

[미리보기]

프롬프트 인젝션 공격, 불안전한 출력 처리, 학습데이터 중독 등 10 가지 보안위협 대응 필요[보안뉴스 김경애 기자] AI 의 바람이 거세지고 있는 가운데, 보안위협 바람도 휘몰아치고 있다. 다크웹을 통해 AI 공격 도구를 판매하거나 AI 를 이용한 악의적 공격으로 기업과 기관을 호시탐탐 노리고 있다. 이에 는 AI 분야 주요 보안위협 10 가지를 살펴봤다. 1.

바로가기

개인정보위, 합법 처리근거 없이 민감정보 수집·활용한 메타 제재... 216 억 과징금 부과

[미리보기]

정당한 사유 없는 열람 거절 및 안전조치 의무 위반 제재도 병행합법 처리 근거 없는 민감정보 수집·활용, 정당한 사유 없는 개인정보 열람 거절 등 3 건 의결[보안뉴스 김영명 기자] 개인정보보호위원회(위원장 고학수, 이하 개인정보위)는 최근 제 18 회 전체회의를 열고 개인정보 보호법(이하 보호법)을 위반한 Meta Platforms, Inc.(이하 메타)에 대

바로가기

---

2. 보안권고문

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-11-04)

[미리보기]

2024-11-25 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. PTZOptics PT30X-SDI/NDI cameras contain an OS command injection vulnerability that allows a remote, authenticated attacker to escalate privileges to root via a crafted payload with the ntp_addr parameter of the /cgi-bin/param.cgi CGI script. 2024-11-04 PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability PTZOptics CVE-2024-8957 2024-11-25 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. PTZOptics PT30X-SDI/NDI cameras contain an insecure direct object reference (IDOR) vulnerability that allows a remote, attacker to bypass authentication for the /cgi-bin/param.cgi CGI script. If combined with CVE-2024-8957, this can lead to remote code execution as root. 2024-11-04 PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability PTZOptics CVE-2024-8956

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