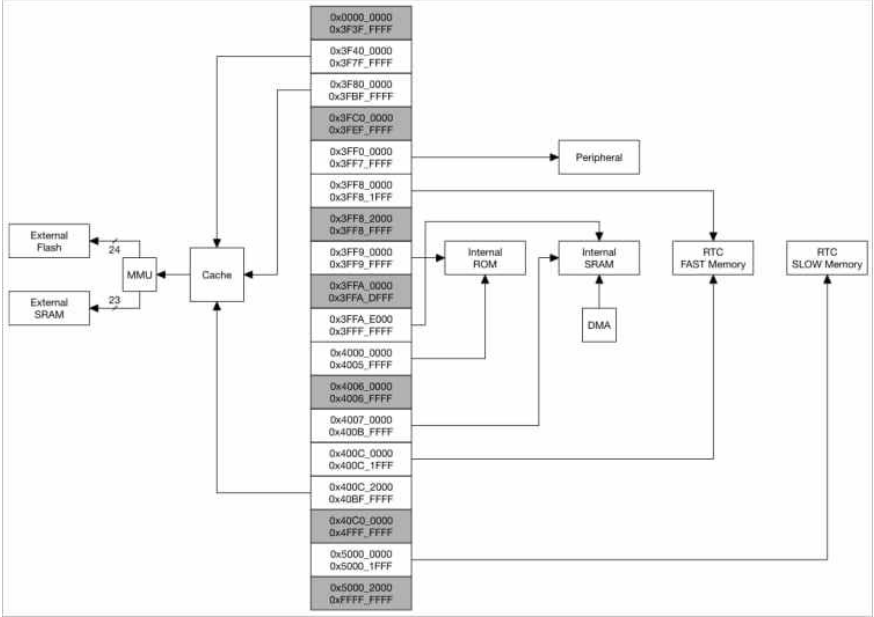


중국산 마이크로 칩, 비공개 명령어 몰래 탑재..전세계 IoT기기 백도어 공격 우려		
날짜/작성자	2025/03/28	김영빈
핵심 내용	<p>스페인 마드리드에서 열린 루티드콘(RootedCON) 행사에서 스페인 연구자 Miguel Tarascó Acuña와 Antonio Vázquez Blanco가 중국 반도체 제조사 에스프레시프(Espressif)의 마이크로칩 'ESP32'에서 제조사가 문서화하지 않은 29건의 명령어를 발견했다고 밝혔다.</p> <p>이 명령어들은 메모리 조작(읽기/쓰기 RAM 및 Flash), MAC 주소 스푸핑(장치 스푸핑), LMP/LLCP 패킷 주입에 사용될 수 있다.</p> <p>연구자들은 ESP32 칩을 완전히 제어하고, RAM 및 Flash 수정 명령어를 통해 칩에 지속성을 얻을 수 있으며, 다른 장치로 확산될 가능성이 있다고 설명하였다.</p>  <p>ESP32 memory map Source: Tarlogic</p> <p>에스프레시프(Espressif)는 이러한 명령어를 공식 문서에 포함하지 않았으므로, 의도치 않게 접근 가능한 기능이거나 실수로 남겨진 것으로 추정. 해당 취약점은 현재 CVE-2025-27840으로 등록되어 추적되고 있다.</p>	

키워드 정리	esp32, 백도어
관련분야	시스템 해킹