

보도 시점 2026. 2. 10.(화) 14:00
(2026. 2. 11.(수) 조간)

배포 2026. 2. 10.(화)

쿠팡 전 직원에 의한 정보통신망 침해사고 조사 결과 발표

- ▷ (조사 범위) △쿠팡 **이용자 인증 체계**, △공격 범위 및 유출 규모 파악을 위한 **접속기록** 등 분석, △전사 차원의 **정보보호 관리체계** 점검
- ▷ (유출 규모)
 - 내정보 수정 페이지 **성명·이메일 3,367만여 건 유출 확인**
 - 배송지 목록 페이지 **1.4억여 회 조회** (성명, 전화번호, 주소 등)
 - 배송지 목록 수정 페이지 **5만여 회 조회** (성명, 전화번호, 주소, 공동현관 비밀번호)
 - 주문 목록 페이지 **10만여 회 조회** (최근 주문한 상품 목록)

※ 개인정보 세부 유출 규모는 개인정보보호위원회에서 확정 예정
- ▷ (사고원인 및 문제점) 공격자는 **이용자 인증 취약점**을 악용하여 정상적인 로그인 없이 이용자 계정에 접속하여 **대규모 정보 무단 유출**
 - 위·변조한 '**전자 출입증**'에 대한 검증 체계가 미흡하여 공격자의 공격 행위를 사전에 탐지·차단하지 못함
 - 모의해킹 결과로 파악한 **보안 취약점 개선 미흡**
 - 공격자가 **이용자 인증 관련 시스템 개발자임에도 퇴사 이후**, 쿠팡은 서명키를 즉시 갱신하지 않은 채 운영
- ▷ (재발 방지 대책) 정상 발급 절차를 거치지 않은 '**전자 출입증**'에 대한 탐지 및 차단 체계 도입, 모의해킹에서 발견한 **취약점 조치 필요**, 서명키 발급·폐기 등 관리체계 강화
- ▷ (조치 사항) 정보통신망법상 **신고 지연**, **자료 보존 명령 위반** 사항 확인
 - (**신고 지연 : 과태료**) 침해사고를 인지한 시점('25.11.17 16:00)으로 부터 **24시간이 지난** 이후 한국 인터넷진흥원(KISA)에 신고('25.11.19 21:35)
 - (**자료 보존 명령 위반 : 수사 의뢰**) 자료 보존 명령('25.11.19 22:34) 이후에도 웹 및 애플리케이션 접속기록을 삭제하여 **조사 제한**

과학기술정보통신부(부총리 겸 과기정통부 장관 배정훈, 이하 “과기정통부”)는 쿠팡 침해사고에 대한 민관합동조사단(이하 “조사단”)의 조사 결과를 2월 10일(화)에 발표하였다.

조사단은 이번 사고에 대해 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”) 제48조의4에 따라 정보통신망에 대한 침해사고의 원인을 분석하고, 유사 사고가 재발하지 않도록 재발 방지 대책을 마련하였다.

한편, 개인정보보호위원회는 개인정보보호법에 따른 개인정보 유출 규모 및 법 위반 여부 등을 조사 중에 있으며, 경찰청은 이번 침해사고와 관련된 증거물 분석 등 수사를 진행 중에 있다. 여타 관련 부처들도 소관 쟁점(이슈)들에 대해 검토 중이라고 과기정통부는 밝혔다.

I. 쿠팡 침해사고 개요

지난 '25.11.16일, 쿠팡은 이용자로부터 개인정보 유출 관련 의심 이메일을 받았다는 내용의 고객의 소리(VOC, Voice Of Customer)를 접수했다.

쿠팡은 자체 조사를 통해 '25.11.17일 침해사고 발생을 인지하고, '25.11.19일 4,536개 계정의 고객명, 이메일, 주소 등 정보가 유출되었다는 내용으로 한국인터넷진흥원(원장 이상중)에 침해사고 신고를 하였다.

※ 정보통신망법상 침해사고 인지 시점으로부터 24시간 이내 신고를 해야 하며, 이를 위반 시 3천만 원 이하 과태료 부과 대상

그러나, 한국 인터넷진흥원이 현장 조사를 통해 추가 피해 여부를 파악한 결과, 유출 규모가 최초 신고된 4,500여 개가 아닌 3천만 개 이상의 계정임이 확인되었다.

과기정통부는 이번 사고가 국내 최대 전자상거래 이음터(플랫폼) 침해사고이며, 대규모 정보가 유출된 중대한 침해사고로 판단하고, '25.11.30일 민관합동조사단을 구성하여 법과 원칙에 따라 피해 현황, 사고원인 등을 조사하였다.

II. 조사 범위

조사단은 공격자가 악용한 쿠팡의 이용자 인증 체계를 정밀 분석하고, 공격 범위 및 유출 규모를 파악하기 위해 웹 및 애플리케이션 접속기록(로그) 등 관련 자료에 대한 종합적인 분석을 실시하였다.

쿠팡으로부터 제출받은 공격자 개인용 컴퓨터(PC) 저장장치(하드 디스크 드라이브<HDD> 2대, 솔리드 스테이트 드라이브<SSD> 2대) 및 현재 재직 중인 쿠팡의 개발자 노트북에 대한 디지털 증거 분석(포렌식 분석)도 병행하였다.

또한, 정보통신망법에 따른 정보보호 조치에 관한 지침, 정보보호 및 개인 정보보호 관리체계인증(ISMS-P) 기준, 쿠팡 자체 규정 등에 대한 준수 여부를 포함해 전사 차원의 정보보호 관리체계를 점검하였다.

III. 정보 유출 규모

공격자는 쿠팡에서 정보를 유출하였다는 이메일을 '25.11.16일, 11.25일 두 차례 쿠팡 측에 보냈으며, 유출한 정보의 일부 내용을 이메일 본문에 기재하였다.

< 공격자가 쿠팡에 보낸 메일('25.11.25, 유출 정보 규모)

(원문)

Hello, due to a not-so-hard-to-find vulnerability in coupang's system, billions of user privacy data items are at significant risk of leak, users from Korea, Japan and Taiwan are impacted. The user data that is identified from various coupang apps and websites in Korea includes:

120+ million pieces of shipping address data

560+ million pieces of order data

33+ million pieces of email address data

(번역)

쿠팡 시스템의 쉽게 발견할 수 있는 취약점으로 인해 수십억 개의 사용자 개인정보 항목이 유출될 위험에 처해 있습니다. 한국, 일본, 대만의 사용자들이 영향을 받고 있습니다. 한국의 다양한 쿠팡 앱과 웹사이트에서 확인된 사용자 데이터는 다음과 같습니다.

1억 2천만 개 이상의 배송 주소 데이터

5억 6천만 개 이상의 주문 데이터

3,300만 개 이상의 이메일 주소 데이터

조사단은 공격자가 유출하였다고 주장하는 이용자 정보들에 대한 사실 여부를 검증하기 위해 쿠팡의 웹 접속기록(로그)을 분석하였다.

그 결과, 조사단은 공격자가 쿠팡의 내정보 수정 페이지의 성명, 이메일, 배송지 목록 페이지의 성명, 전화번호, 주소, 공동현관 비밀번호 정보, 주문 목록 페이지의 이용자가 주문한 상품 정보를 유출한 후, 해당 정보 일부를 이메일에 기재하여 쿠팡 측에 보낸 것을 확인하였다.

※ 개인정보 유출 : 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나, 제삼자가 그 내용을 알 수 있는 상태에 이르게 된 것(표준 개인정보보호 지침)

< 공격자가 쿠팡에 보낸 메일('25.11.25, 주문 상품 정보) >

```
email: [REDACTED].com
user: [REDACTED]
addresses:
#1: [REDACTED] | 경기도 안산시 [REDACTED] | 010-[REDACTED] | (문앞, 문앞(원형버튼+열 [REDACTED]))
#2: [REDACTED] | 경기도 안산시 [REDACTED], [REDACTED] | 010-[REDACTED] | (문앞, )
recent orders:
#1: 2025. [REDACTED] | 11, [REDACTED]원 | 1개 | [REDACTED] 생리대 날개형 중형 16p x 3개 + 대형 14p, [REDACTED]트
#2: 2025. [REDACTED] | 17, [REDACTED]원 | 일부상품이분리되어배송됩니다 | [REDACTED] 생수, 2L, [REDACTED]개
#3: 2025. [REDACTED] | 17, [REDACTED]원 | 1개 | [REDACTED] 생수, 2L, 18개
#4: 2025. [REDACTED] | 17, [REDACTED]원 | 분리배송된상품입니다 | [REDACTED] 생수, 2L, [REDACTED]개
#5: 2025. [REDACTED] | 2, [REDACTED]원 | 1개 | [REDACTED] 스마트폰 거치대 6.5x11x12.5~16.5 cm, 화이트, [REDACTED]대
#6: 2025. [REDACTED] | 13, [REDACTED]원 | 분리배송된상품입니다 | [REDACTED] 생리대 수퍼롱 날개형, 오버나이트 이상, 20개입, [REDACTED]대
#7: 2025. [REDACTED] | 6, [REDACTED]원 | 1개 | [REDACTED] 아령, 1kg, [REDACTED]대
#8: 2025. [REDACTED] | 0원 | 1개 | [REDACTED] 돌기 폼롤러 45cm, 스카이블루, 45x14cm, [REDACTED]대

sample data in 대구광역시 [REDACTED]
email: [REDACTED].com<mailto:[REDACTED].com>
user: [REDACTED]
addresses:
#1: [REDACTED] | 대구광역시 [REDACTED], [REDACTED] | 010-[REDACTED] | (직접받고부재시문앞, 문앞([REDACTED]))
#2: [REDACTED] | 부산광역시 [REDACTED], [REDACTED] | 010-[REDACTED] | (직접받고부재시문앞
#3: [REDACTED] | 대구광역시 [REDACTED], [REDACTED] | 010-[REDACTED] | (문앞, 문앞(없음))
#4: [REDACTED] | 대구광역시 [REDACTED], [REDACTED] | 010-[REDACTED] | (기타사항([REDACTED]
recent orders:
#1: 2025. [REDACTED] | 6, [REDACTED]원 | 1개 | [REDACTED] 자른당면, 500g, [REDACTED]대
#2: 2025. [REDACTED] | 17, [REDACTED]원 | 1개 | 통셀러리, 500g, [REDACTED]개
#3: 2025. [REDACTED] | 3, [REDACTED]원 | 1개 | 국내산 양파, 1.5kg, [REDACTED]개
#4: 2025. [REDACTED] | 17, [REDACTED]원 | 1개 | 통셀러리, 500g, [REDACTED]개
#5: 2025. [REDACTED] | 16, [REDACTED]원 | 1개 | [REDACTED] 생리대 날개형, 대형, 16개입, [REDACTED]대
#6: 2025. [REDACTED] | 17, [REDACTED]원 | 1개 | [REDACTED] 생리대 날개형, 중형, 18개입, [REDACTED]대
#7: 2025. [REDACTED] | 12, [REDACTED]원 | 1개 | 통셀러리, 500g, [REDACTED]대
#8: 2025. [REDACTED] | 4, [REDACTED]원 | 1개 | 국내산 브로콜리, 2개입, [REDACTED]대
#9: 2025. [REDACTED] | 30, [REDACTED]원 | 1개 | [REDACTED] 수입 레몬 효능 칼로리 국내산 성분 1kg, [REDACTED]스,
#10: 2025. [REDACTED] | 12, [REDACTED]원 | 1개 | 통셀러리, 500g, [REDACTED]대
#11: 2025. [REDACTED] | 2, [REDACTED]원 | 1개 | 표고버섯, 200g, [REDACTED]대
#12: 2025. [REDACTED] | 1, [REDACTED]원 | 1개 | 국내산 청양고추, 150g, [REDACTED]개
#13: 2025. [REDACTED] | 3, [REDACTED]원 | 1개 | 국내산 양파, 1.5kg (대), [REDACTED]개
```

또한, 쿠팡 웹 및 애플리케이션 접속기록(로그) 데이터 분석을 통해, 내정보 수정, 배송지 목록, 주문 목록 등 페이지에서 쿠팡의 이용자 정보가 유출되었음을 확인하였다.

내정보 수정 페이지에서 성명, 이메일이 포함된 이용자 정보 33,673,817건이 유출되었음을 확인하였다.

<내정보 수정 페이지(예시)>

계정 보호를 위해 본인 인증이 필요합니다

계정 보호를 위해, 비밀번호를 입력해야 회원정보 수정이 가능합니다. 기존 회원정보는 인증 과정에서 변경/삭제되지 않습니다.

아이디(이메일)

비밀번호

[비밀번호 찾기](#)

성명, 전화번호, 배송지 주소, 특수문자로 비식별화된 공동현관 비밀번호가 포함된 배송지 목록 페이지에 148,056,502회 조회*하여 정보가 유출되었음을 확인하였다. 배송지 목록 페이지에는 계정 소유자 본인 외에도 가족, 친구 등 제3자의 성명, 전화번호, 배송지 주소 등 정보가 다수 포함되어 있다.

* 상기 정보가 포함된 배송지 목록 페이지를 방문한 횟수를 의미

<배송지 목록 페이지(예시)>

MY 배송지

주문목록/배송조회
취소/반품/교환/환불
내역
와우 멤버십
구독 서비스
로켓프레시 프레스백
영수증 조회/출력

MY 혜택
쿠폰 - 이용권
쿠팡캐시/기프트카드

MY 활동
문의하기
문의내역 확인
리뷰관리
찜 리스트

MY 정보
개인정보확인/수정
결제수단-쿠팡이 관리
배송지 관리
회원 탈퇴

김[redacted]
(기본배송지) (로켓프레시 가능) (로켓와우 가능)
서울특별시 강남구 [redacted]호
010-88[redacted]
일반: 문 앞 (#1****) / 새벽: 문 앞 (#1****)

김[redacted]
(로켓프레시 가능) (로켓와우 가능)
대구광역시 수성구 [redacted]호
010-88[redacted]
일반: 문 앞 / 새벽: 문 앞 (경비실 호출)

김[redacted]
(로켓프레시 가능) (로켓와우 가능)
경기도 파주시 목동 [redacted]호
010-28[redacted]
일반: 문 앞 / 새벽: 문 앞 (경비실 호출)

그리고, 성명, 전화번호, 배송지 주소 외에 공동현관 비밀번호가 포함된 배송지 목록 수정 페이지를 50,474회 조회했음을 확인하였다.

<배송지 목록 수정 페이지(예시)>

MY쿠팡	쿠팡이머니	0원	쿠팡캐시
MY 쇼핑 주문목록/배송조회 취소/반품/교환/환불 내역 와우 멤버십 구독 서비스 1 로켓프레시 프레시백 1 영수증 조회/출력	김 [redacted] 서울특별시 강남구 [redacted] 81 KR +82 10-88 [redacted] 일반 : 문 앞 (#10 [redacted]) 새벽 : 문 앞 (#10 [redacted]) ☒ 기본 배송지로 선택 저장 삭제		
MY 혜택 쿠폰 - 이용권 쿠팡캐시/기프트카드			
MY 활동 문의하기 문의내역 확인 리뷰관리 1 찜 리스트			
MY 정보 개인정보확인/수정 결제수단·쿠팡이머니 관리 배송지 관리 회원 탈퇴			

또한, 이용자가 최근 주문한 상품 목록이 포함된 주문 목록 페이지를 102,682회 조회하였음을 확인하였다.

<주문 목록 페이지(예시)>

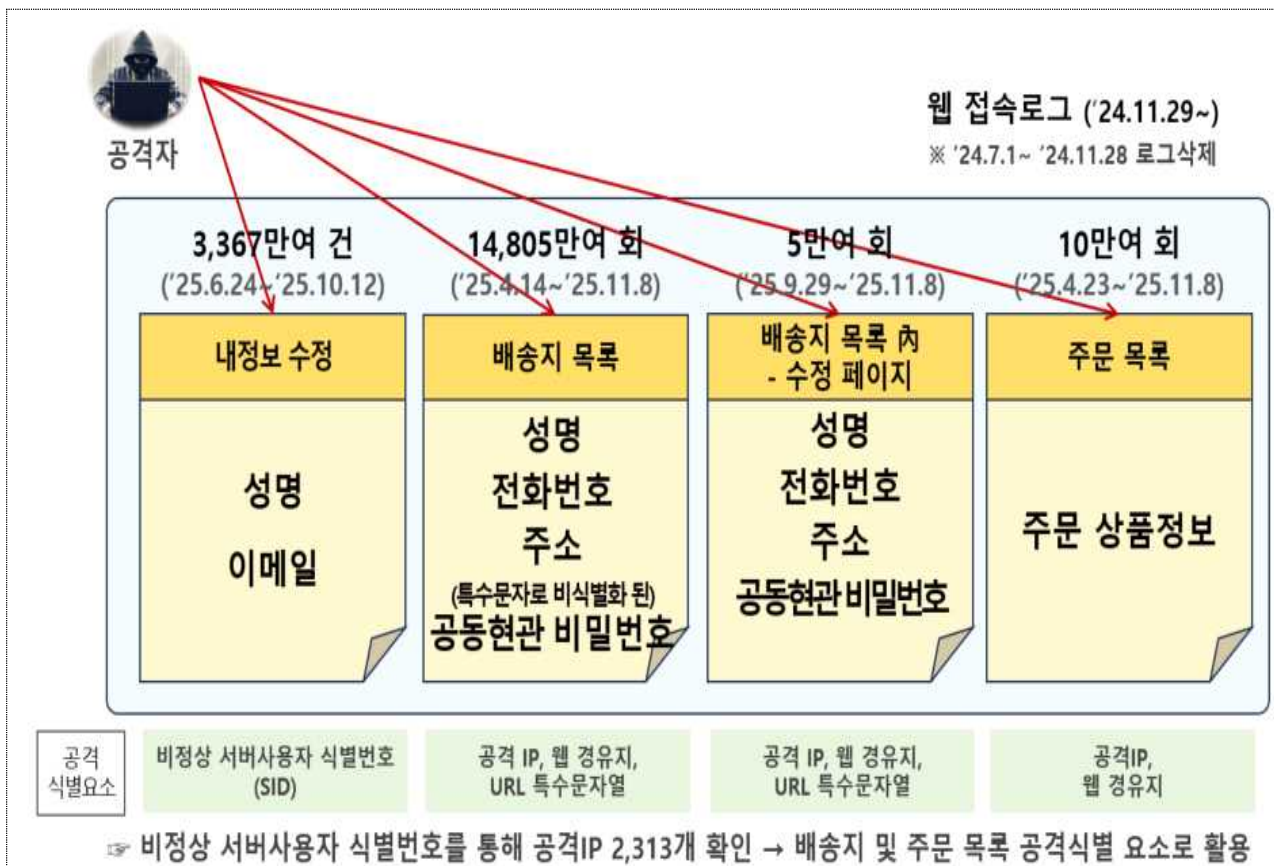
MY쿠팡	쿠팡이머니	0원	쿠팡캐시	0원
MY 쇼핑 주문목록/배송조회 취소/반품/교환/환불 내역 와우 멤버십 구독 서비스 1 로켓프레시 프레시백 1 영수증 조회/출력	주문목록 주문한 상품을 검색할 수 있어요! 최근 6개월 2026 2025 2024 2023 2022 2021			
MY 혜택 쿠폰 - 이용권 쿠팡캐시/기프트카드	2025. 8. 24 주문 배송완료 · 8/24(일) 도착 일부 상품이 분리되어 배송됩니다 분리 배송 로켓프레시 핫반 백미밥, 210g, 30개 28,790 원 1개 장바구니 담기	주문 상세보기 > 배송 조회 교환, 반품 신청		
MY 활동 문의하기 문의내역 확인 리뷰관리 1 찜 리스트	배송완료 · 8/24(일) 도착 분리배송된 상품입니다 분리 배송 로켓프레시 핫반 백미밥, 210g, 30개 28,790 원 1개 장바구니 담기	배송 조회 교환, 반품 신청		
MY 정보 개인정보확인/수정 결제수단·쿠팡이머니 관리 배송지 관리 회원 탈퇴				

조사단은 웹 접속기록 등을 기반으로 유출 규모를 산정하였으며, 향후 개인정보 유출 규모에 대해서는 개인정보보호위원회에서 확정하여 발표할 예정이다.

〈 정보 유출 규모 분석결과〉

- (분석 대상 및 범위) 쿠팡 접속기록(로그) 용량 25.6 테라바이트(TB)
 - 분석 데이터 저장기간 : 24.11.29 ~ 25.12.31
 - 분석 데이터 규모 : 6,642억 건(664,256,750,511건)
 - (분석 결과) 25.4.14 ~ 25.11.8 기간에 걸쳐 공격한 것으로 확인되었으며, 해당 웹페이지에 접속하여 **이용자 정보를 유출한 것으로 판단**
 - ※ 공격자가 쿠팡에 접속 시 특정 서버 사용자 식별번호를 사용하여 이용자 계정에 접속한 사실이 확인되어, 이를 참고하여 접속로그 내 공격자 인터넷 프로토콜(IP), 유입경로(Referer) 등 조사
- ① **내정보 수정 페이지** : 33,673,817건 * 성명, 이메일
 - ② **배송지 목록 페이지** : 148,056,502회 조회 * 성명, 전화번호, 주소, 특수문자로 비식별화된 공동현관 비밀번호
 - ③ **배송지 목록 內 수정 페이지**: 50,474회 조회 * 성명, 전화번호, 주소, 공동현관 비밀번호
 - ④ **주문 목록 페이지** : 102,682회 조회
- ※ 개인정보 유출 규모는 개인정보보호위원회에서 최종 확정 예정

< 쿠팡의 정보 유출 규모 분석력과 >

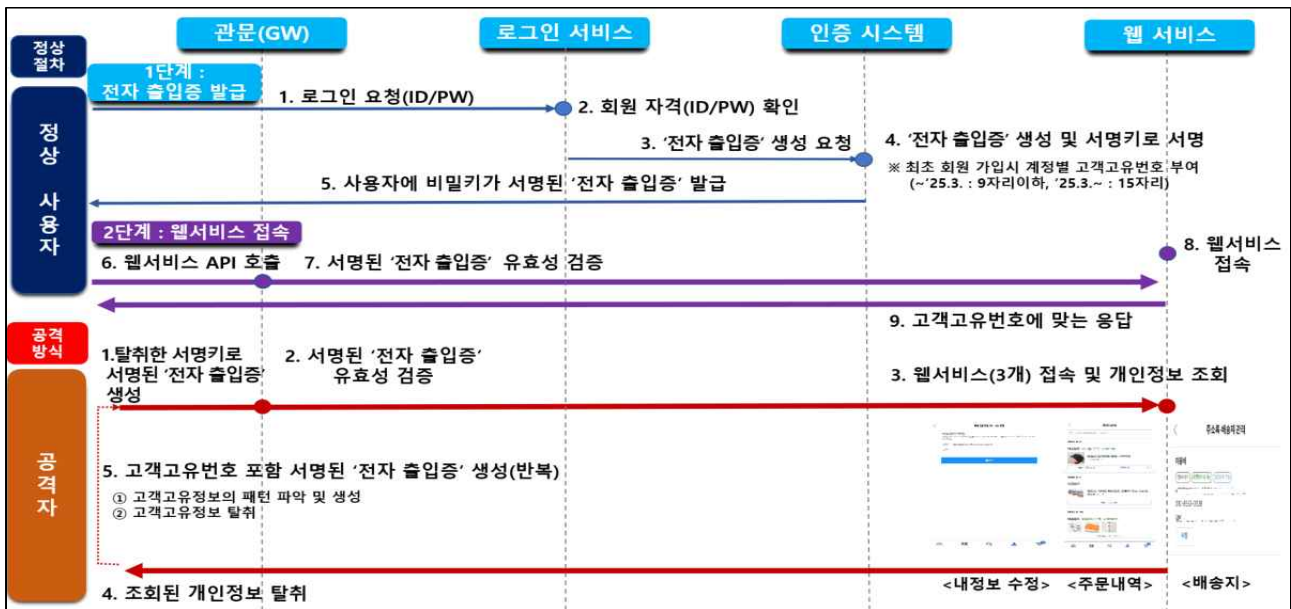


IV. 사고원인 분석

조사단은 사고원인을 정보 유출 경로 분석, 공격자 행위 분석 두 가지 측면에서 조사하였다.

※ 공격자는 재직 당시 시스템 장애 등 백업을 위한 이용자 인증 시스템 설계·개발 업무를 수행한 소프트웨어 개발자(Staff Back-end Engineer)로 확인됨

< 유출경로 분석 >



조사단은 정보 유출 경로를 분석한 결과, 공격자가 쿠팡 서버의 인증 취약점을 악용하여 정상적인 로그인 없이 이용자 계정에 비정상 접속하여 정보를 무단 유출했음을 확인하였다.

정상적으로 이용자가 접속하는 경우, 이용자는 로그인(ID/PW) 절차를 거쳐 일종의 '전자 출입증'을 발급받는다. 그리고, 쿠팡의 관문 서버는 발급받은 '전자 출입증'이 유효한지 여부를 검증하고, 이상이 없을 시에 서비스 접속을 허용한다.

공격자는 재직 당시 관리하던 이용자 인증 시스템의 서명키를 탈취한 후, 이를 활용해 '전자 출입증'을 위·변조하여 쿠팡 인증 체계를 통과하였다. 그 결과, 정상적인 로그인 절차를 거치지 않고 쿠팡 서비스에 무단 접속할 수 있게 되었다.

< 공격자 행위 분석 >

① 취약점 발견 단계(25.1월 이전)

공격자는 재직 당시, 이용자 인증 시스템 설계·개발 업무를 수행하면서, 이용자 인증 체계의 취약점과 키 관리체계의 취약점을 인지하고 있었다.

※ (판단 근거) 공격자가 25.1.5~1.20 공격 시험(테스트)을 진행한 접속기록이 확인되었기에, 1월 이전에 취약점을 인지하고 있었다고 판단

먼저, 쿠팡의 관문 서버는 인증 절차를 통해 ‘전자 출입증’이 정상적으로 발급된 이용자에 한해서 접속을 허용해야 하므로, ‘전자 출입증’이 위·변조되었는지에 대해서도 확인해야 한다. 하지만 조사 결과, 관련된 확인 절차가 부재한 상황이었다.

또한, 쿠팡이 관리하는 서명키는 ‘전자 출입증’을 발급하기 위해 사용하는 도구인 만큼, 체계적이고 엄격한 관리체계를 갖추어야 한다. 이에, 업무 담당자가 퇴사할 경우 해당 서명키를 더 이상 사용하지 못하도록 갱신 절차가 진행되어야 하나, 관련 체계 및 절차가 미비하였다.

② 취약점을 악용한 공격 시험(테스트)(25.1월~)

퇴사 후, 공격자는 재직 당시 탈취한 서명키와 내부 정보를 활용하여, ‘전자 출입증’에 대한 위·변조를 진행하였다. 그 후, 이를 이용해 정상적인 로그인 절차 없이 쿠팡 인증 체계를 통과하면서, 본격적인 공격을 위한 사전 시험(테스트)을 진행하였다.

< 조사단 확인 내용 >

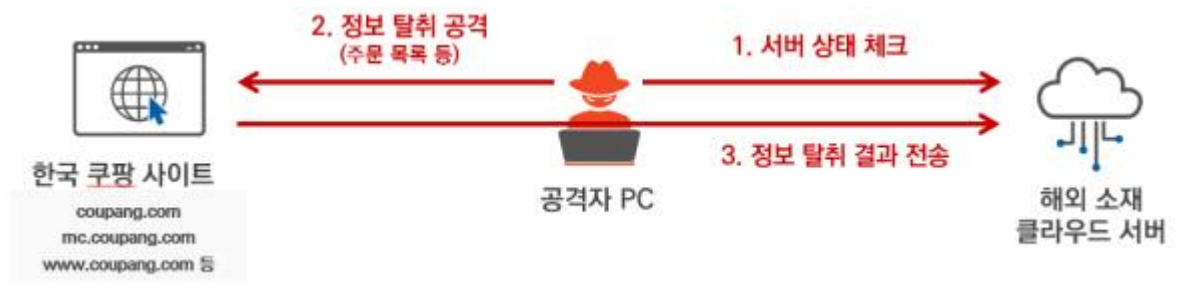
- ▶ 현재 재직 중인 개발자 노트북 포렌식 결과, 서명키를 키 관리 시스템에서만 저장해야 함에도 불구하고, 개발자 노트북에 저장(하드코딩)한 사실 확인
- ▶ 공격자 개인용 컴퓨터(PC) 저장장치(하드 디스크 드라이브<HDD> 2대, 솔리드 스테이트 드라이브<SSD> 2대) 포렌식 결과, 쿠팡에서 사용하고 있는 이용자 고유식별번호 및 위·변조 ‘전자 출입증’ 확인
- ▶ ‘25.4.14~11.8 기간 동안 공격을 진행하기 이전에, 25.1월 경 공격 흔적 확인

③ 대규모 정보 유출(25.4.14~11.8)

공격자는 사전 시험(테스트)을 통해 이용자 계정에 접근이 가능한 사실을 확인한 이후, 자동화된 웹크롤링 공격 도구를 이용하여 대규모 정보를 유출하였다. 이 과정에서 공격자는 총 2,313개 인터넷 규약 주소(IP)를 이용하였다.

< 조사단 확인 내용 >

- ▶ 조사단은 공격자 PC 저장장치(하드 디스크 드라이브<HDD> 2대, 솔리드 스테이트 드라이브<SSD> 2대)를 디지털 증거 분석(포렌식 분석)한 결과, 공격자가 **정보 수집 및 외부 서버 전송**이 가능한 **공격 스크립트**를 작성한 것 확인
- 또한, 위·변조 ‘전자 출입증’을 이용해 타인의 계정으로 무단 접속한 후 유출한 정보(주문 목록 등)를 **해외 소재의 인터넷 기반 자원 공유(클라우드) 서버로 전송할 수 있는 기능 확인**
- ※ 다만, 실제 전송이 이루어졌는지 여부에 대해서는 기록이 남아있지 않아 확인할 수 없음



V. 문제점 및 재발 방지 대책

조사단은 조사를 통해 쿠팡의 정보보호 체계에 문제점을 발견하고 재발 방지 대책을 마련하였다.

< 이용자 인증 체계 문제점 >

조사단은 공격자가 위·변조한 ‘전자 출입증’을 사용하여 쿠팡 서비스에 무단으로 접속한 것을 확인하였고, 정상적인 발급 절차를 거친 ‘전자 출입증’인지 여부를 검증하는 체계가 부재한 사실을 확인하였다.

또한, 쿠팡은 모의해킹을 통해 ‘전자 출입증’ 기반 인증 체계의 취약점 발굴·개선을 추진하였으나, 발견된 문제에 한하여 해결책을 모색하고, 쿠팡의 관문 서버 이용자 인증 체계 개선 등 전반적인 문제점 검토는 이루어지지 않았다.

⇒ (재발 방지 대책) 쿠팡은 정상 발급 절차를 거치지 않은 ‘전자 출입증’에 대한 탐지 및 차단 체계를 도입하는 한편, 모의해킹에서 발견된 취약점에 대해서는 근본적인 문제개선 방안을 마련하여야 한다.

< 키 관리체계 문제점 >

쿠팡은 자체 규정에 따라, 서명키를 ‘키 관리 시스템’에서만 보관하고, 개발자 개인용 컴퓨터(PC) 등에 저장(소스 코드 내 하드코딩) 하지 않도록 해야 한다고 명시하고 있다. 그러나, 조사단은 현재 재직 중인 쿠팡 개발자가 노트북에 서명키를 저장하고 있어, 키 유출 및 오남용 위험이 있음을 발견하였다.

또한, 쿠팡은 서명키를 체계적으로 관리할 수 있도록 발급 내역을 기록·관리하도록 규정하고 있으나, 조사단은 키 이력 관리체계가 부재하여 목적 외 사용을 파악하는 것이 불가능함을 확인하였다.

쿠팡은 내부자(퇴사자)로 인하여 서명키와 같은 주요 정보가 탈취될 수 있는 위험에 대한 대응체계가 부재하였다.

이와 함께, 조사단은 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)에 대해서 점검한 결과, 쿠팡은 개발과 운영을 분리하지 않고 개발자에게 실제 운영 중인 ‘키 관리 시스템’에 접근하도록 권한을 부여하고 있었다. 그리고, 내부 규정에서 키의 수명(3년 주기)만 정의하였고, 사용자의 정보 변경에 따른 교체 등 세부적인 운영 절차 수립이 미흡하였다.

⇒ (재발 방지 대책) 쿠팡은 키 관리(발급/사용 이력 관리)·통제 체계 강화 및 운영관리 기준을 명확히 하고, 상시 점검을 시행해야 한다.

< 정보보호 관리체계 미흡 >

쿠팡은 이번 침해사고가 동일한 서버 사용자 식별번호*를 반복적으로 사용했으며, 위·변조된 ‘전자 출입증’을 활용한 비정상 접속 행위가 발생했음에도, 해당 공격 행위를 통한 정보 유출을 탐지·차단하지 못했다.

* 웹 서버가 다수의 웹페이지 요청자를 구별하기 위하여 각 세션에 부여하는 임의의 문자열 값 또한, 접속기록(로그)을 일관된 기준 없이, 저장·관리하여 피해 이용자 식별 및 정보 유출 규모 산정에 어려움이 발생하였다.

※ 쿠팡은 접속기록(로그) 중 서버 사용자 식별번호, 이용자 고유식별번호를 내정보 수정 페이지에서만 저장·관리하고 있으며, 배송지 목록, 주문 목록 등 페이지에서는 해당 정보를 저장·관리하고 있지 않음

⇒ (재발 방지 대책) 쿠팡은 비정상 접속 행위 탐지 점검(모니터링)을 강화하고, 사고원인 분석 및 피해 규모 식별 등 목적에 맞는 로그 저장관리 정책을 수립 및 정비하여야 한다. 또한, 자체 보안규정 준수 여부에 대한 정기 점검을 실시하고, 미준수 사항 발생 시 즉각 개선하는 관리체계를 구축하여야 한다.

< 법 위반 사항 >

① 침해사고 신고 지연

쿠광은 정보통신망법 제48조의3에 따라 침해사고를 인지한 후 24시간 이내에 과기정통부 또는 한국 인터넷진흥원(KISA)에 신고하여야 한다. 그러나, 정보보호 최고책임자(CISO)에게 보고한 시점('25.11.17 16:00)으로부터 24시간이 지난 후 한국 인터넷진흥원(KISA)에 신고('25.11.19 21:35) 하였다.

※ **(침해사고 인지 시점)** 침해사고 발생을 알게 된 때는 정보보호 담당자, 정보보호 담당 부서의 장, 정보보호 최고책임자, 기업 대표자 등이 정보통신망법 제2조에 정의된 침해사고의 발생을 알게 된 때를 말한다.(정보통신 분야 침해사고 대응 안내서, '25.8월)

⇒ **(조치 사항)** 정보통신망법에 따른 과태료를 부과할 예정이다.

※ 정보통신망법 제76조에 따라 3천만 원 이하 과태료 부과 대상

② 자료 보존 명령 위반

과기정통부는 정보통신망법 제48조의4에 따라 쿠광에 침해사고 원인 분석을 위해 자료 보존을 명령('25.11.19 22:34)하였다.

그러나, 쿠광은 자료 보존 명령에도 불구하고 자사 접속기록의 자동 로그 저장 정책을 조정하지 않아, 약 5개월('24.7~11월) 분량 웹 접속기록이 삭제되었다. 또한, 애플리케이션 접속기록(로그)도 '25.5.23~6.2일 간의 데이터가 삭제되었다.

⇒ **(조치 사항)** 자료 보존 명령 위반과 관련하여 수사기관에 수사를 의뢰하였다.

※ 웹 로그 삭제 : 수사 의뢰(25.12.31) / 애플리케이션 로그 삭제 : 수사 의뢰(26.2.9)

VI. 향후 계획

과기정통부는 이번 조사단의 조사 결과를 토대로, 쿠광에 재발 방지 대책에 따른 이행계획을 제출(2월)토록 하고, 쿠광의 이행(3~5월) 여부를 점검(6~7월)할 계획이다. 이행점검 결과, 보완이 필요한 사항에 대해서는 정보통신망법 제48조의4에 따라 시정조치를 명령할 계획이다.

담당 부서	과학기술정보통신부 사이버 침해조사팀	책임자	과장	김우철 (044-202-6490)
		담당자	사무관	김성환 (044-202-6491)
		담당자	사무관	김재남 (044-202-6493)
관련 기관	한국인터넷진흥원 위협분 석단	책임자	단장	박용규 (02-405-4800)
		담당자	팀장	김홍석 (02-405-4830)