infosec

Threat Intelligence Report

EQST INSIGHT

2022

02

EQST(이큐스트)는 'Experts, Qualified Security Team'
이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된
최고 수준의 보안 전문가 그룹입니다.

infosec

Contents

EQST insight

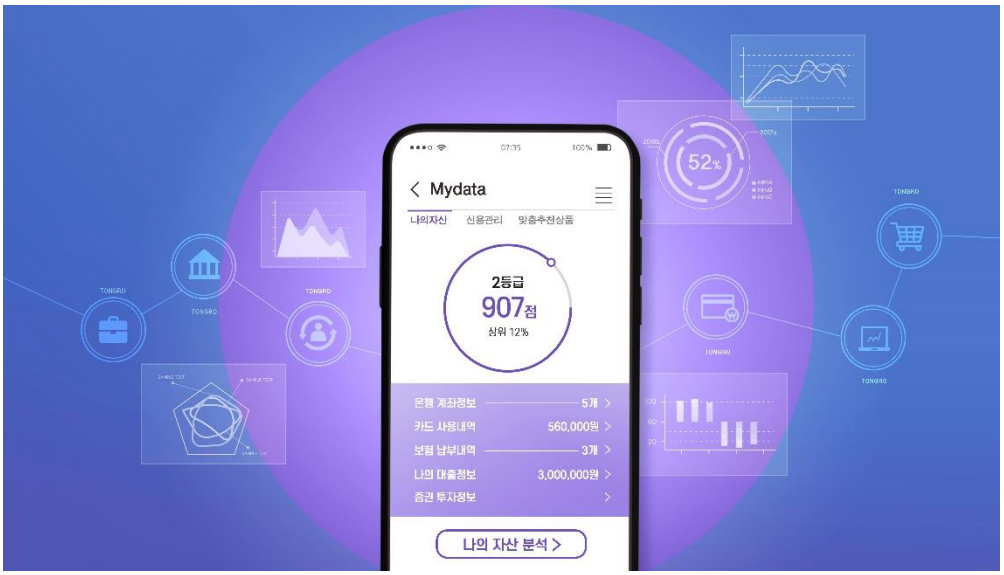
마이데이터 서비스 본격화에 따른 마이데이터 사업자 보안 위협 분석 및 보안 대응 전략

1. 마이데이터 서비스, 개인신용정보 활용 본격화

2021년에 “신용정보의 이용 및 보호에 관한 법률”(이하 “신용정보법”) 개정으로 올해부터 다양한 마이데이터 서비스가 출현하며 정보주체인 소비자의 개인신용정보 활용이 본격적으로 시작되었다.

마이데이터 서비스는 기존 금융 서비스와 달리 컴플라이언스 및 규제 기관의 가이드라인 요건에 맞게 구축되어야 하는 특성을 가지고 있기 때문에 다양한 업권의 금융회사들은 서비스를 출시하며 수많은 시행착오를 겪었다. 막상 힘겹게 서비스를 오픈했지만 시장 초기 마이데이터 사업자 간의 가입자 유치 경쟁으로 인해 커피 쿠폰을 제공하는 기업의 매출이 증가하고 있다는 일부 언론 기사가 간혹 눈에 띄기도 했다. 이와 같이 2021년에는 서비스 오픈을 위해 분주했다면, 올해는 개인신용정보 활용을 통해 이윤을 창출하는 방안을 모색하기 위한 각 금융회사의 다양한 마케팅 연구가 지속될 것으로 보인다.

다만 안정적인 서비스 운영 및 고도화를 위해서는 최신 컴플라이언스를 준수하고, 개인신용정보 유출 등 각종 사이버 침해 공격을 예방하기 위한 강화된 보안 체계와 대응 전략 수립이 필요할 것으로 보인다. 이러한 상황에 발맞춰 SK쉴더스는 보안 관점에서 마이데이터 서비스의 현재 상황과 보안 위협 및 강화된 법령 등을 살펴보고, 서비스 보안 체계 고도화를 위한 방안을 모색해보고자 한다.



2. 금융회사 마이데이터 사업자 현황

`22년 1월 현재 마이데이터 사업자로 본허가를 받은 기업은 55개사, 예비허가 7개사, 허가신청 19개사이며 허가를 받기 위한 기업들은 지속적으로 늘어날 전망이다.

infosec

업권	본허가(55개사)	예비허가(7개사)	허가신청(19개사)
은행	국민은행, 농협은행, 신한은행, 우리은행, SC제일은행, 하나은행, 광주은행, 전북은행, 중소기업은행, 대구은행 (10개사)	-	카카오뱅크 (1개사)
보험	교보생명, KB손해보험 (2개사)	신한생명, 미래에셋생명 (2개사)	메리츠화재, 흥국화재해상보험 (2개사)
금융투자	미래에셋대우, 하나금융투자, 한국투자증권, 키움증권, NH투자증권, KB증권, 현대차증권 (7개사)	교보증권, 신한금융투자 (2개사)	하이투자증권, 대신증권, 한화투자증권 (3개사)
여신 전문금융	국민카드, 우리카드, 신한카드, 현대카드, BC카드, 현대캐피탈, 하나카드, KB캐피탈, 롯데카드 (9개사)	-	-
상호금융	농협중앙회 (1개사)	-	-
저축은행	웰컴저축은행 (1개사)	-	동양저축은행 (1개사)
CB사	나이스평가정보, 코리아크레딧뷰로 (2개사)	-	SCI평가정보 (1개사)
핀테크	네이버 파이낸셜, ㈜핀테크, 카카오페이, 토스, 핀크, NHN페이코, SK플래닛, 민앤지, 뱅크샐러드, 뱅큐, 보맵, 쿠콘, 팀윙크, 핀다, 한국금융솔루션, 해빗팩토리, 아이지넷, 디셈버앤컴퍼니자산운용, 유비벨록스, 애프앤가이드, 코드에프, 한국신용데이터 (22개사)	HN핀코어, 기웅정보통신 (2개사)	오라인포, 웰스가이드, 인공지능연구원(AIRI), 코나아이 SCI평가정보, 차이코퍼레이션, 패스트포워드, 다날 (7개사)
기타	LG CNS (1개사)	피플펀드컴퍼니 (1개사)	SK텔레콤 11번가, KT, LGU+ (4개사)

< 마이데이터 허가 현황(`22년 1월 기준, 신용정보협회 홈페이지) >

마이데이터 업권 별 사업자들의 비즈니스 모델을 살펴보면 아래와 같다.

(1) 은행권 : 개인 자산관리 고도화에 중점을 둔 다양한 생활편의성을 제공하는 등의 종합 금융 플랫폼 지향

(2) 금융투자권 : 금융투자권은 맞춤형 자산관리 컨설팅과 빅데이터 분석, 인공지능(AI) 기술을 활용한 투자 진단 서비스 등 차별화된 서비스를 제공

(3) 카드권 : 새로운 비즈니스 기회 창출을 위해 소비패턴 분석에 기반하여 생활 서비스&금융 플랫폼으로 영역네 확대를 모색하는 등 현재의 결제 및 카드 금융 중심의 사업에서 벗어나 새로운 데이터 기반의 종합 생활금융 플랫폼 기반 구축

(4) 보험권 : 보험권은 인허가 자격 이슈, 비즈니스 모델 검토 중으로 아직 2개 사업자만이 본허가를 받았다. 사업모델은 보험 통합조회, 보장 분석, 일상생활 보험 판매, 건강 분석 등 다양한 서비스로 영역을 확장할 예정

(5) 핀테크 : 기존의 스크린 스크레이핑 기술 기반 서비스의 제공 등 기업간편결제업의 영역을 넘어 종합 플랫폼 비즈니스 선점을 위해 타 사업자들과 경쟁

※ 스크린 스크레이핑 : 공인인증서 등 본인 확인 수단을 정보주체로부터 위탁받아 정보를 수집하는 방식

3. 마이데이터 서비스 보안 위협

개인맞춤형 금융서비스인 마이데이터 서비스는 양질의 개인정보를 다량 보유하고 있어 불특정 다수의 공격 대상이 되기 쉬우므로 마이데이터 플랫폼 또는 API 연계 지점 등을 노리는 공격이 증가할 것으로 보인다.

마이데이터 사업자는 마이데이터 플랫폼의 관문이 되는 API의 보안 강화(지속적 인증 도입, 보안성 갖춘 API 중개자 선정, API Gateway 접근통제 강화 등)와 함께 공격자 관점의 플랫폼 공격 시나리오와 TTP(전술·기술·절차) 분석 등 고도의 인텔리전스 역량을 갖출 필요가 있다.

※ API(Application Programming Interface) : 마이데이터 사업자와 정보제공자 간 개인신용정보를 송수신하기 위한 미리 정의된 표준화된 전송규격 및 절차

infosec

보안 위협	취약점 발생 요인	보안 대책
마이데이터 사업자의 IT인프라의 취약점을 이용한 사이버 공격	개인의 금융자산, 거래내역 등 중요한 개인신용정보가 집중되어 있는 마이데이터 인프라의 취약점 개선노력 미흡	- 서비스 출시 전 사전보안성 검토 - 시스템 취약점 진단 및 조치 - 접근통제 시스템 구축 및 고도화
암호화되지 않은 개인정보의 대량 유출로 인한 사회 경제적 막대한 피해 발생	개인정보 암호화 등의 개인정보 유출 대책 미흡	- 본인인증 절차 강화 - 개인정보 처리(출력, 전송, 저장 등)시 안전한 암호화 알고리즘 적용
마이데이터 사칭(피싱, 스미싱 등) 웹/앱에 의한 인증 정보 탈취로 고객의 금전적 피해 발생 및 각종 사이버범죄 악용 가능성	서비스 이용자의 보안수칙 준수 미흡	- 서비스 이용자에 대한 보안 인식 제고 활동 - 이용자의 보안수칙 준수

< 마이데이터 서비스의 보안 위협과 대응 방안 >

위에서 열거한 다양한 보안 위협의 대응을 위해 마이데이터 사업자는 보안성 검토, 취약점 진단 등 기본적인 보안 대책을 통해 전자금융기반시설에 준하는 보안 수준을 확보해야 한다.

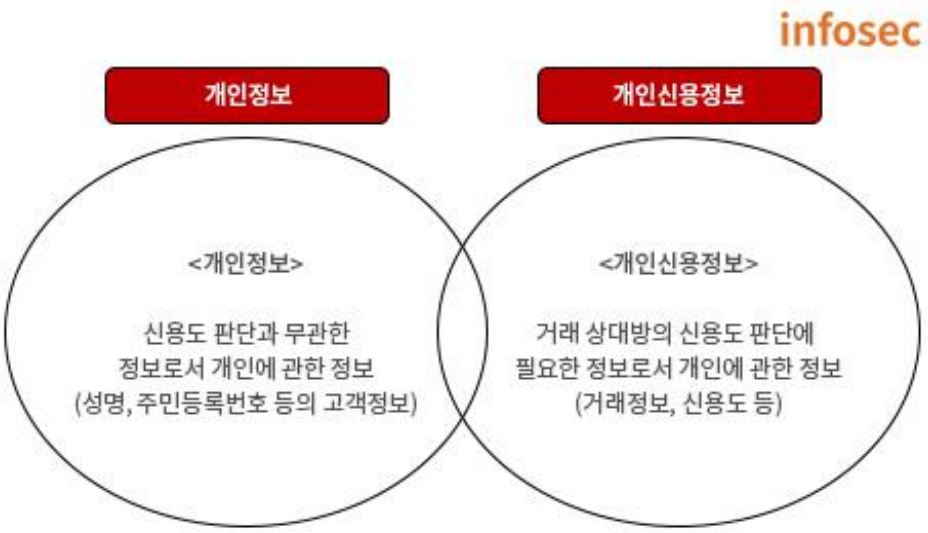
infosec

보안 대책 종류	세부 내용
보안성 검토	자체 보안성심의 평가항목 기반 현황 점검 - 관리·물리·기술 영역 진단 - 취약점에 대한 이행조치 확인 등
취약점 진단	마이데이터 인프라 대상 취약점 진단 - 서버, DB, 네트워크, 미들웨어, 정보보호시스템 - 웹·앱 어플리케이션 등
서비스 수준 평가	마이데이터 관련 법령 및 가이드 준수 현황 점검 - 마이데이터 관련 법령 - 마이데이터 서비스 가이드라인 - 마이데이터 기술 가이드라인 등

< 마이데이터 서비스 기본 보안 대책 >

4. 개인정보보호법 과징금 부과, 마이데이터 사업자도 예외일 수 없어

국내의 개인정보 이동권은 신용정보법에 국한된 개인신용정보에 한해서 이동권을 적용하여 금융 서비스 산업의 데이터유통 활성화 측면을 강조하는 반면, GDPR(유럽연합 개인정보보호규정)의 개인정보이동권은 정보주체의 권리 보장 측면에서 개인정보 전체(개인신용정보 포함)를 대상으로 하고 있다.



< 개인정보와 개인신용정보 >

다만 금융회사의 데이터활성화 측면과는 별개로 과징금 부과 기준을 GDPR(유럽연합 개인정보보호 규정) 수준에 맞춰 '전체 매출액의 3%'로 상향하는 개인정보보호법 전면 개정안이 21년 9월 30일 국회에 제출되어 현재 법안 통과를 위해 대기 중이다. 개정안이 발효될 경우 각 사업자들은 개인신용정보를 포함하여 개인정보의 안정성 확보 조치 미흡으로 인한 과징금 제재를 받지 않기 위해 개인정보 관련 서비스의 보안 대책 마련이 시급해 보인다. 특히, 마이데이터 서비스는 다량의 개인정보를 전송 및 제공하는 만큼 더욱 철저한 대비가 필요하다.

infosec

No	개정 내용	비고
1	과징금 전체 매출의 3%로 일원화 과징금 3% 부과되는 경우 1개에서 11개로 10개 내용 신설	신설
	과실에 대한 형사처벌 폐지	폐지
2	기존 정보통신사업자에서 모든 처리자 대상 정보유출 등의 침해사고 발생 시 손해배상책임이행보험 의무화	개정
3	과징금 부과 근거가 되는 중대한 침해사고 판단기준 8가지 제시	신설

< 개인정보보호법 개정안 주요 내용 >

개인정보보호위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우 해당 개인정보처리자에게 전체 매출액의 3% 이하에 해당하는 금액으로 과징금을 부과한다는 내용을 개정안에 명시하였다.

마이데이터 사업자는 개정안의 내용 중 제29조(안전조치의무) 항목의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치에 관한 사항 등 사전에 대비할 수 있는 항목에 대한 안전 조치를 강화할 필요가 있다.

infosec

No	조항	과징금 부과 사유
1	제15조(개인정보의 수집·이용) 제1항	해당 조항을 위반하여 개인정보를 처리한 경우
⋮	⋮	⋮
9	제29조(안전조치의무)	안전성 확보에 필요한 조치가 미흡한 경우
⋮	⋮	⋮
11	제37조(개인정보의 처리정지 등) 제2항	개인정보를 계속 이용하거나 이를 제3자에게 제공한 경우

< 전체 매출의 3% 과징금이 부과 주요 내용 >

개정안에는 과징금 부과 시 고려사항을 명시하여 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 하였다. 즉, 위반행위의 정도와 안전성 확보 조치 노력 등에 따라 과징금을 차등 부과할 수 있도록 한 것이다.

infosec

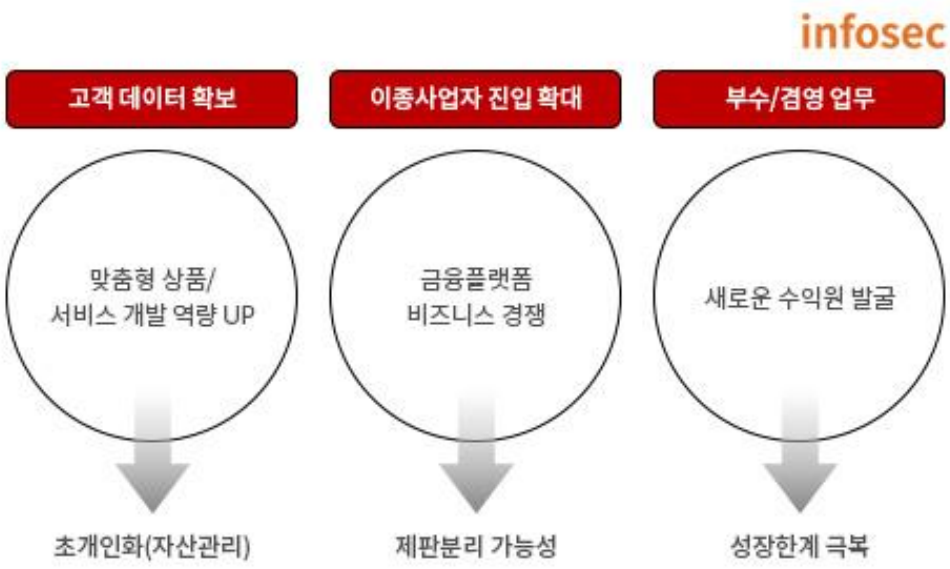
No	조항	세부내용
1	64조의2 제3항	암호화등 안전성 확보에 필요한 조치 이행 노력 정도
2		개인정보가 분실·도난·유출·위조·변조 또는 훼손된 정도 및 안전성 확보 조치 등 의무 위반행위와의 인과관계
3		개인정보처리자의 업무 형태 및 규모
4		처리하는 개인정보의 민감도
⋮		⋮

< 개인정보보호법 개정안 과징금 부과 시 주요 고려사항 >

5. 마이데이터 서비스 보안 대응 전략

마이데이터 서비스의 본격 도입에 따른 긍정적인 측면으로는 정보주체인 고객이 개인신용정보 전송요구권을 바탕으로 다양한 데이터를 활용하여 개인화·맞춤화된 새로운 금융서비스를 마이데이터 사업자로부터 제공받을 수 있게 된다.

금융산업의 측면에서는 기존 주요 금융회사의 고객 데이터 독점이 해소되면서 시장 지배력이 약화되고, 시장 경쟁이 치열해짐에 따라 금융분야의 개방형 혁신이 본격적으로 추진될 것으로 예상된다.



< 마이데이터 사업의 영향 및 시사점 – (보험연구원 2021) >

부정적인 측면으로는 마이데이터 서비스가 새로운 금융 플랫폼의 안정적인 수익원으로 자리잡으려면 신용정보법, 개인정보보호법 등 강화된 컴플라이언스를 준수하고 금융회사에 내재되어 있는 보안 취약점을 지속적으로 개선할 수 있도록 보안 체계 고도화 등의 보안 대책이 동반되어야만 할 것이다.

SK쉴더스에서는 마이데이터 사업자들이 보안체계 수립을 통한 서비스 경쟁력 및 신뢰도를 확보할 수 있도록 사업 준비, 구축 및 운영 단계에서 필요한 보안 컨설팅과 관제 서비스 및 적합한 솔루션을 제안한다.

서비스 종류		세부 내용
보안 컨설팅	인허가 준비 컨설팅	서비스 준비 및 허가 단계에서 시스템 및 보안체계 구성 등에 대한 물적요건 대응
	기능적합성 심사 사전 대응 및 보안성검토 컨설팅	서비스 구축 단계에서 관련 컴플라이언스, 가이드 기준 충족 및 서비스 오픈 전 취약점 개선
	보안취약점 점검 컨설팅	서비스 운영과정에서 발생 가능한 취약점 도출 및 개선
	정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 컨설팅	데이터 종류 및 보유량에 따른 개인정보 흐름 파악, 취약점 도출 및 개선대책 수립
	마스터플랜수립 컨설팅	개인신용정보 안전성 확보조치에 대한 중·장기 보호대책 마련
보안 관제	모니터링	마이데이터서비스 인프라 접속이력 모니터링 등
	유해 트래픽 탐지	개인정보 처리 이상징후 관련 탐지 등
보안 솔루션	금융 컴플라이언스 준수	서버보안, 접근통제, 계정관리솔루션 등
	개인정보보호 특화	내부통제강화 솔루션, 개인정보 Life-Cycle 관리 솔루션, 고객(정보주체) 권리보장을 위한 솔루션 등

< SK쉴더스 마이데이터 관련 서비스 >

2022년 개인정보보호법 개정으로 신용정보법 기반의 금융회사뿐만 아니라 정보주체의 개인정보 이동권이 금융권 이외의 전체 업종으로 확대될 예정이다. 마이데이터 서비스의 종류에 따라 이동되는 개인정보의 양이 상당해지는 만큼 대규모 개인정보 침해 사고의 발생 위험 또한 커질 것으로 보인다.

SK쉴더스는 마이데이터 서비스가 본격화되고 있는 시점에서 보안 전문가의 다양한 노하우와 기술력을 바탕으로 마이데이터 사업자의 고객 정보 지킴이이자 든든한 버팀목이 되고자 한다

6. 참고문헌

- 개인정보 보호법 일부 개정안(2021. 9. 28, 의안번호 12723)
- 2022년 디지털금융 및 사이버보안 이슈전망(2022. 01. 금융보안원)
- 금융 마이데이터 도입 현황과 시사점(2021. 04. 보험연구원)
- 본인신용정보관리업(마이데이터) 신규허가 현황(2021. 10. 금융보안원)
- 마이데이터 국내외 현황 및 주요 해외 사례(2021. 03. KDB산업은행)
- 신용정보의 이용 및 보호에 관한 법률
- 금융분야 마이데이터 기술 가이드라인
- 금융분야 마이데이터 서비스 가이드라인
- 금융분야 마이데이터 표준API 규격 등

Special Report

심스와핑(SIM Swapping) 공격을 통한 가상 자산 탈취, 대응 방안은?

■ 개요

최근 국내에서 네 차례 연달아 심스와핑(SIM Swapping) 공격[1] 의심 사례가 발생했다. 피해자는 가상화폐거래소를 이용하던 개인이며 피해 규모는 2억 8000만 원에 달한다. 심스와핑 공격은 해외에서는 간혹 발생하던 공격이었지만 국내에서 2021년 12월경 최초로 발생했다. 이후 일부 가상화폐거래소에서 계정 해킹 및 출금을 시도한 정황을 포함해 심스와핑 의심 사례가 잇달아 발생하자 불안감이 커지고 있는 상황이다.

이번 Special Report에서는 심스와핑을 통한 가상 자산 탈취 시나리오를 유추하고 심스와핑이 가지는 파급력과 대응 방안에 대해 알아보고자 한다.

[1] 사용자를 식별하는 유심을 복제해 휴대전화를 이용한 본인 인증을 통과하는 방식으로 타인의 금융자산이나 가상 자산을 탈취하는 공격

■ 국내에서 발생한 심스와핑 의심 사례

심스와핑 공격으로 의심되는 4건의 국내 피해 사례를 살펴보면 공격자는 심스와핑을 통해 피해자의 SNS, 포털 비밀번호를 변경하고 2차 인증을 무력화했다. 최종적으로는 피해자의 가상화폐거래소 계정을 획득하여 해당 계정이 보유하고 있는 가상 자산을 노렸음을 알 수 있다.

infosec

분류	일자	증상 및 피해내용
사례 1	2021년 12월 23일 (IOS)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. SNS, 포털 비밀번호 타인에 의해 재설정 3. 다음날 동일 증상(유심 기변 기록) 4. 가상자산 타인 계좌로 무단전송(약 100만원 피해)
사례 2	2022년 1월 12일 (Android)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. 피해자가 재부팅 시도했으나 증상 반복 3. SNS, 포털 비밀번호 타인에 의해 재설정 4. 피해자가 해킹 의심되어 스마트폰 전원 종료 5. 가상자산 무단 유출 확인(약 2200만원 피해)
사례 3	2022년 1월 16일 (Android)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. SNS, 포털 비밀번호 타인에 의해 재설정 3. 당일 대리점 방문하여 유심정지 조치 4. 가상화폐거래소 자체 의심거래 차단(피해 없음)
사례 4	2022년 2월 12일 (알 수 없음)	1. 가상자산 무단 유출 확인(약 2억 6000천만원 피해) 2. 스마트폰 통신 불가 증상(유심기변 기록) 3. 유심변경 메시지 및 SNS 타 기기 로그인 내역 확인

■ 국내 심스와핑 의심 사례 분석

1. 복제된 유심에 의한 공격

언론의 보도에 따르면 국내에서 발생한 심스와핑 의심 사례는 복제된 유심에 의한 공격일 가능성이 높은 것으로 보인다. 공격자가 어떤 방식으로 유심을 복제했는지는 알려지지 않았지만, 해외에서 발생한 심스와핑 사례에서 유심 복제 방법은 크게 두가지로 분류할 수 있다.

첫 번째 방법은 다크웹에서 구매한 개인정보로 이동통신사를 속여 유심을 발급받는 것이다. 다크웹에서는 해킹을 통해 유출된 개인정보가 활발하게 유통되고 있기 때문에 이름, 연락처를 포함한 불특정 다수의 개인정보를 쉽게 획득할 수 있다. 이러한 정보를 이용하여 이동통신사에 유심 분실, 파손을 이유로 피해자를 가장해 재발급을 신청할 수 있으며, 발급과정에 적절한 본인확인 절차가 없는 경우 제3자의 유심 발급이 가능하다. 해외에서는 이동통신사의 허술한 보안 정책을 악용하여 유명인을 대상으로 심스와핑 공격이 이루어진 사례가 다수 존재한다. 또한 최근 스페인에서는 소셜 엔지니어링 기법[2]으로 통신사 직원들을 속여 심카드를 복제한 일당이 체포된 사례가 있다.

두 번째 방법은 이동통신사 내부 직원을 매수하여 유심을 복제하는 것이다. 2019년 미국에서 발생한 사례로, 이동통신사 직원이 대가를 받고 유심 발급에 필요한 개인정보를 공격자에게 제공했다. 공격자는 이를 이용하여 여러 피해자의 유심을 발급받아 공격에 악용하여 약 200만 달러 이상의 피해가 발생했다.

[2] 소셜 엔지니어링 기법 : 기술적인 해킹 기법을 사용하는 대신 사람의 심리를 악용해 시스템 또는 데이터, 건물에 대한 출입 권한을 확보하는 해킹 수법으로, 사회공학적 공격이라고도 함

2. 심스와핑 공격을 통한 가상 자산 탈취

국내에서 발생한 심스와핑 의심 사례에서 공격자의 최종 목표는 모두 피해자의 가상 자산이었다.

infosec

분류	증상 및 피해내용
사례 1	약 100만원의 자산이 무단으로 이더리움으로 환전 되고 타인의 가상 지갑으로 전송됐다.
사례 2	피해자가 휴대전화를 잠시 꺼둔 사이 가상화폐거래소에서 2,200만원가량의 가상자산이 탈취됐다.
사례 3	공격자가 피해자의 가상자산 계좌를 노렸으나, 거래소에서 자체적으로 크리덴셜 스터핑을 시도하는 계정으로 인지하고 출금 제한으로 전환되어 가상자산 출금에 실패했다.
사례 4	피해자의 약 2억 6000만원 상당의 가상자산이 무단으로 전량 매도한 후 클레이튼(KLAY)을 매수되어 다른 지갑으로 출금되었다.

위 사례들을 통해 공격자가 피해자의 가상화폐거래소 계정과 해당 계정이 보유하고 있는 가상 자산을 목표로 한다는 것을 알 수 있다. 가상 자산은 흔적이 남지 않고 추적이 어렵기 때문에 최근 공격자들이 선호하는 공격 목표다.

※ 가상 자산을 노리는 심스와핑 공격자 동향은 해외 사례로도 확인할 수 있다.

- 2018년 8월, 미국의 가상 자산 투자자가 통신사 직원의 정보 유출로 인해 2380만 달러 상당의 심스와핑 피해를 입었다고 주장하며 이동통신회사를 고소

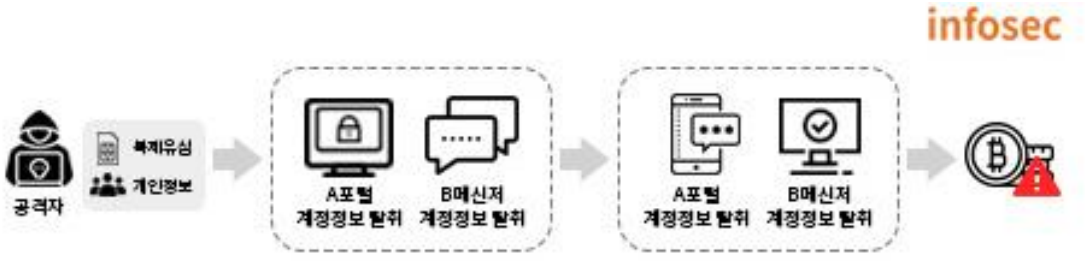
- 2021년 4월, 메사추세츠에서 심스와핑을 통해 10명 이상의 SNS 계정을 탈취하고 가상 자산 53만 달러 이상을 탈취하려 시도했지만 검거

- 2021년 11월, 캐나다 온타리오 주에서 10대 청소년이 심스와핑을 통해 가상 자산 3650만 달러를 탈취하여 검거

- 2021년 한 해 동안 FBI가 접수한 심스와핑 공격은 1611건이며, 총 피해액은 6800만 달러에 달함

■ 심스와핑 공격 시나리오

공격자는 심스와핑을 시도할 수 있는 복제 유심과 피해자의 개인정보(이름, 전화번호, 생년월일)을 획득한 후, 가상화폐거래소에서 계정 인증수단으로 사용되는 주요 포털 또는 메신저의 '아이디 찾기', '비밀번호 재설정' 기능을 이용해 계정정보 탈취를 시도한다. 심스와핑 공격을 통해 본인인증 우회가 가능하여 피해자의 계정정보 획득이 가능하고, 이후 동일한 방법으로 피해자의 가상화폐거래소 계정에 접근할 수 있으며 가상 자산을 탈취할 수 있다.



[심스와핑 발생 시 가상 자산 탈취 시나리오]

1. 공격자는 공격에 필요한 복제 유심(심스와핑)과 공격 대상의 개인정보 일부를 획득

2. 가상화폐거래소에서 계정 인증수단으로 사용되는 A포털과 B메신저의 계정을 탈취 시도

- A 포털 심스와핑 통해 '계정찾기', '비밀번호재설정', '2차인증 해제'로 계정정보 탈취
- B 메신저 심스와핑 통해 '계정찾기', '비밀번호재설정'로 계정정보 탈취

3. C가상화폐거래소 계정 획득

- 심스와핑 통해 '비밀번호 찾기' 기능으로 1차 인증 획득
- 심스와핑 통해 'OTP 재발급' 통한 2차 인증 획득

4. 피해자의 가상화폐거래소 계정 접근 및 가상 자산 탈취

■ 심스와핑 공격 대응 방안

1. 유심(USIM) 비밀번호 설정

유심은 스마트폰 사용자를 인증하는 수단으로 사용될 수 있기 때문에 이를 악용한다면 금전적인 피해로 이어질 수 있다. 이러한 공격을 방지하는 방법은 유심에 비밀번호를 설정하는 것이다. 유심기변을 시도할 때마다 설정한 비밀번호를 입력해야 하기 때문에 타인이 무단으로 유심을 사용하는 것을 방지할 수 있다. 다만 공격자가 피해자의 개인정보를 훔쳐 별도의 유심을 발급한 경우 유심 비밀번호로는 공격을 막을 수 없다.

※ 초기 유심 카드 비밀번호는 0000(4개) 또는 00000000(8개)이며 제품과 제조사에 따라 상이할 수 있다. 또한 비밀번호 3회 이상 틀릴 경우 유심이 잠기므로 무리하게 시도하지 말아야 한다.

2. 엠세이퍼(M-Safer) - 이동전화 가입 제한 서비스 이용

한국정보통신진흥협회(KAIT)에서 운영 중인 엠세이퍼(www.msafer.or.kr)를 이용하면 개인정보 유출에 의한 유심 발급을 방지할 수 있다. 엠세이퍼에서는 '이동전화 가입제한 서비스', 'SMS 및 이메일 안내 서비스'를 제공하고 있다. 이동전화 가입제한 서비스는 통신사 별로 신청해야 하는 가입제한을 일괄적으로 처리해 주는 서비스이며 명의 도용에 의한 이동전화 신규 가입 및 명의변경을 사전에 차단할 수 있다. 또한 SMS 및 이메일 안내 서비스는 본인의 명의로 이동전화가 개통되는 경우 SMS 또는 이메일로 알람을 받을 수 있어 무단 개통이 발생하는 경우 빠르게 조치할 수 있다.

3. 심스와핑 의심 시 가상화폐거래소 계정 잠금 요청 및 유심 이용정지 신청

아침 시간에 스마트폰이 갑자기 먹통이 되거나, 메신저 또는 메일에 타인에 의한 계정 상태 변경 기록이 남아 있다면 심스와핑 공격을 의심할 수 있다.

심스와핑 공격은 주로 이른 새벽 시간대에 발생하며, 복제 유심이 타 기기에 삽입되어 인증되는 경우 피해자가 기존에 사용하던 스마트폰은 정상적인 통신이 불가한 상태가 된다. 만일 메일 또는 메신저에 제3자에 의한 계정 탈취를 시도한 흔적이 남아 있다면 즉시 가상화폐거래소의 계정 잠금 기능을 이용하여 로그인과 출금을 막아야 한다. 국내 사례에서 확인할 수 있듯 공격자는 최종적으로 피해자의 가상 자산을 노리고 있다. 공격자의 목표가 가상 자산인 만큼 자신이 사용하는 가상화폐거래소의 계정 잠금 설정 방법을 숙지하고 있는 것이 좋다.

또한 심스와핑을 인지한 즉시 이동통신사 고객센터를 통해 이용정지를 신청하는 것이 추가적인 피해를 막을 수 있는 방안이다. 다만 개인정보를 탈취하여 명의를 도용한 경우 피해자가 기존에 사용하던 통신사가 아닌 다른 통신사에서 개통될 가능성도 존재한다. 따라서 엠세이퍼(www.msafer.or.kr)에서 '가입사실 현황조회 서비스'를 이용하여 개통된 유심을 확인하고 아래 도표의 통신사별 고객센터에 문의하여 유심 이용정지를 신청해야 한다.

분류	SKT	KT	LGU+	LG헬로비전	KCT	세종텔레콤	알뜰폰
무료	114, 080-011-6000 (유선)	114, 080-000-1618	114, 080-019-7000	070-7373-1002~3 (LG헬로비전 이용자)	080-1300-114	080-880-9300	각 통신사별 문의
유료	1599-0011	1588-0010	1544-0010	1855-1144	1877-9115	1688-9300	-

■ 참고 URL

https://m.boannews.com/html/detail.html?mtype=1&idx=104183
https://m.boannews.com/html/detail.html?mtype=1&idx=104097
https://m.boannews.com/html/detail.html?mtype=1&idx=103915
https://www.hankookilbo.com/News/Read/A2022021515400003908
https://cointelegraph.com/news/sim-swapping-how-hackers-stole-millions-worth-of-crypto-via-victims-telecoms-operator
https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-operating-nationwide-scheme-steal-social-media-accounts-and
https://www.abcactionnews.com/money/consumer/taking-action-for-you/cybercriminals-cleanout-cryptocurrency-using-sim-card-swap-scam
https://www.pcmag.com/news/canadian-teen-arrested-for-sim-swap-attack-that-looted-36-million
https://post.naver.com/viewer/postView.naver?volumeNo=33149073&memberNo=36310338&vType=VERTICAL
https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/
https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-sim-swapping-criminal-ring
https://www.vice.com/en/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam
https://www.boannews.com/media/view.asp?idx=104785
https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169

HTTP 프로토콜 스택 원격 코드 실행 취약점 (CVE-2022-21907)

■ 취약점 개요

2022년 1월, 마이크로소프트의 첫 번째 정기 패치에 포함된 취약점인 'CVE-2022-21907'은 공격자가 HTTP 프로토콜 스택(http.sys)을 활용하여 원격 코드를 실행할 수 있는 취약점이다. HTTP 프로토콜 스택은 Windows 구성 요소 중 하나로 HTTP 요청을 고속으로 처리하는 데 사용되는 커널 모드 장치 드라이버이며 HTTP 요청에 대한 구문 분석 및 클라이언트로 보낼 응답 생성을 담당한다. 해당 취약점은 HTTP 요청 헤더의 Accept-Encoding 값을 구문 분석하는 과정에서 서비스 거부 공격 및 원격 코드 실행으로 이어진다.

현재까지 악용된 사례는 보고되지 않았으나 마이크로소프트 취약성 지수(Microsoft Exploitability Index)에 따르면 '악용 가능성이 높음(Exploitation More Likely)' 평가를 받았고, 인증되지 않은 공격자가 HTTP 프로토콜 스택을 사용하여 패킷을 처리하는 서버에 악의적으로 조작된 패킷을 보낼 수 있어 CVSS[3] 10점 만점 중 9.8점의 높은 점수를 받았다. 또한, 워머블(wormable)한 특성이 있어 네트워크를 통한 자가 전파가 가능하기 때문에 더욱 주의가 필요하다.

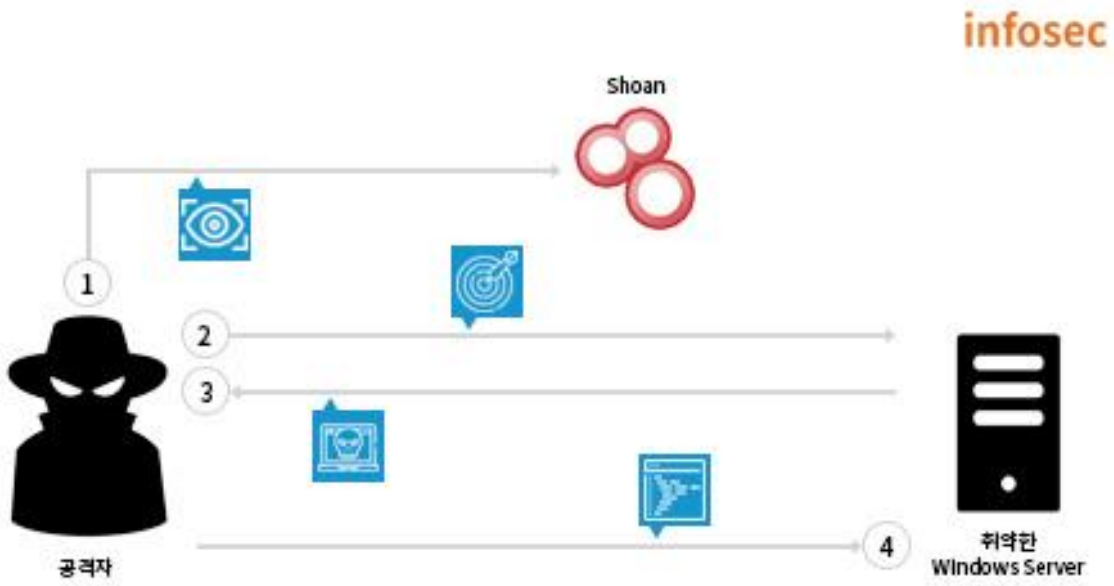
■ 영향 받는 소프트웨어 버전

CVE-2022-21907에 취약한 소프트웨어는 다음과 같다.

S/W 구분	취약 버전
Windows	Windows 10 Version 2004 Windows 10 Version 1809, 20H2, 21H2 Windows 11 Windows Server 2019, 2022, 20H2

[3] Common Vulnerability Scoring System 으로 공통 취약점 등급 시스템을 의미함.

■ 공격 시나리오



[공격 시나리오]

① Shodan과 같은 검색 엔진을 활용하여 취약한 버전의 Windows를 사용하고 있는 대상 탐색
② CVE-2022-21907 PoC를 통한 공격 진행
③ 서비스 거부 및 피해자 PC 제어권 탈취
④ 원격 코드 실행

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2022-21907의 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 Version 2004 (build 19041.264) 192.168.0.128
공격자	Windows 10 Version 21H1 192.168.0.1

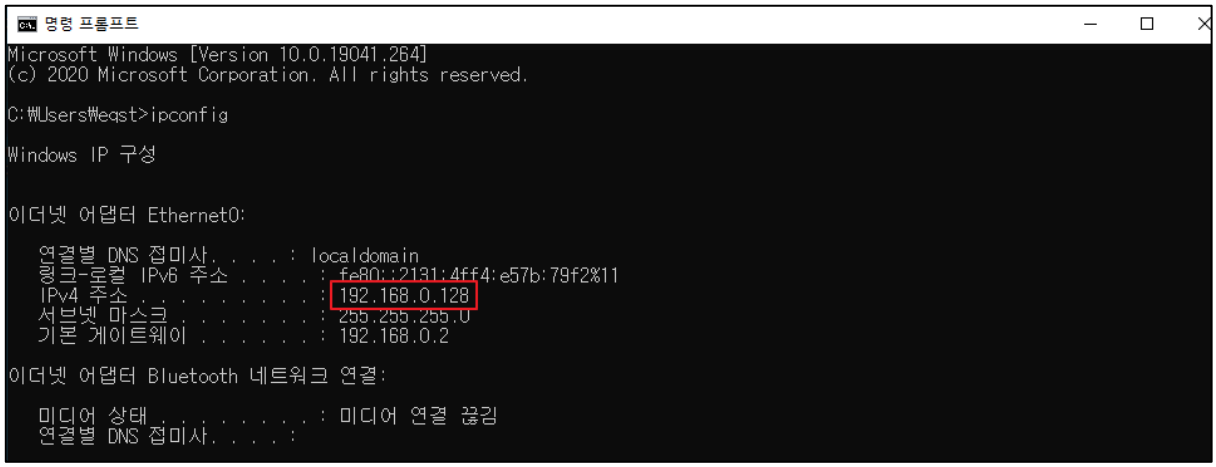
■ 취약점 테스트

Step 1. 환경구성

step 1) CVE-2022-21907은 HTTP 프로토콜 스택(http.sys)의 취약점으로 이를 사용하는 서비스[4]로 환경구성[5]을 해야 한다. 이번 인사이트에서는 취약한 버전의 Windows 10 Version 2004 설치 후 IIS 서버를 구성했다.

[취약한 Windows 버전 정보]

step 2) 공격 대상인 피해자 PC 의 IP 주소를 ipconfig 명령어를 통해 확인한다.

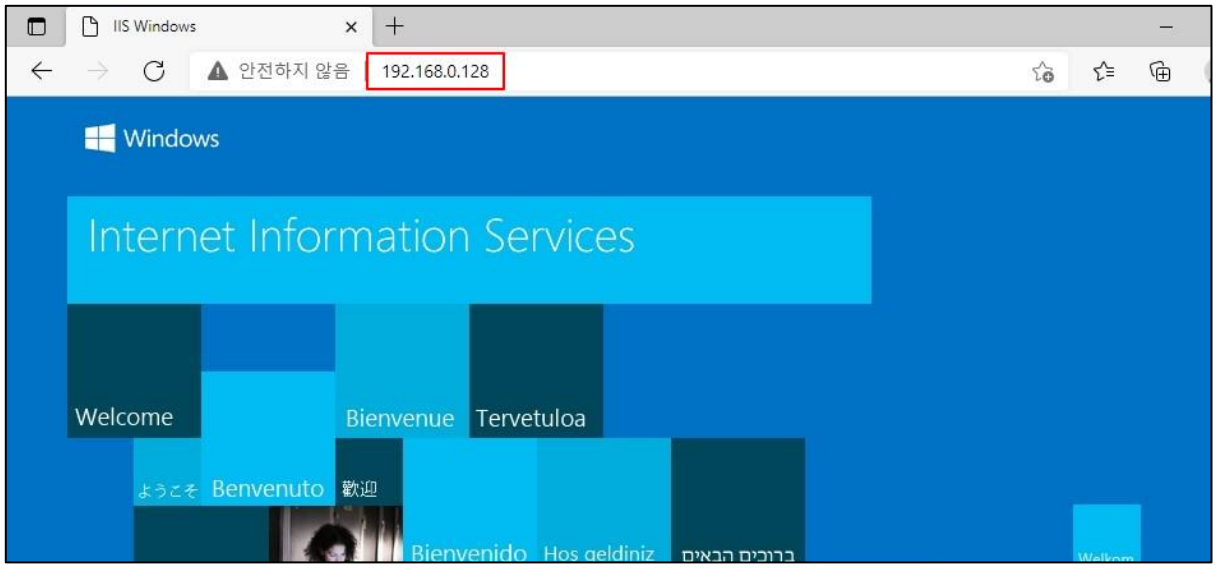


[피해자 IP 주소]

[4] http.sys 를 사용하는 서비스에는 IIS 서버를 비롯해 WinRM, WSDAPI 등이 있다.

[5] IIS 서버 활성화는 프로그램 및 기능 > Windows 기능 켜기/끄기 > 인터넷 정보 서비스 > 웹 관리 도구 > IIS 관리 콘솔 선택으로 가능하다.

step 3) IIS 서버가 실행되고 있는지 접속해 본다.



[피해자 PC의 IIS 서버]

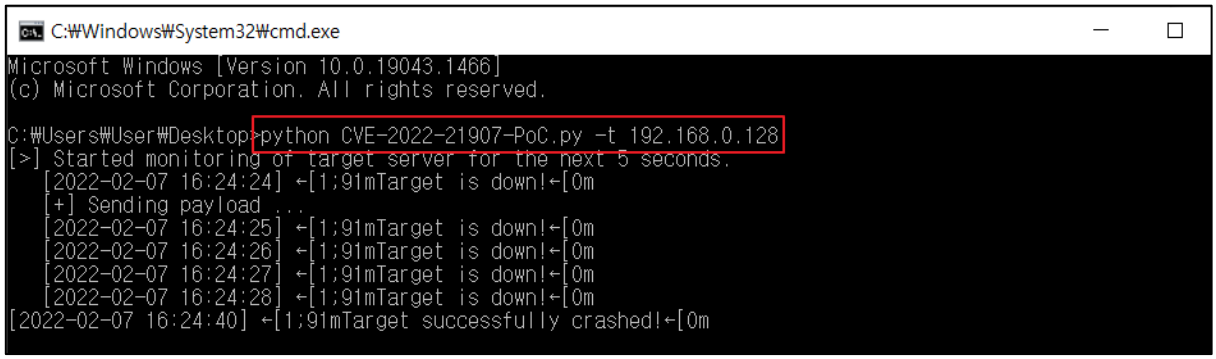
Step 2. PoC 테스트

테스트를 위한 PoC가 저장된 github URL은 다음과 같다.

URL : https://github.com/p0dalirius/CVE-2022-21907-http.sys

step 1) 공개된 PoC를 이용해 공격자 PC에서 공격을 시도한다.

명령어는 아래와 같으며 -t 옵션에 공격 대상의 IP 주소를 입력한다.



[PoC 실행]

step 2) 공격 성공 시 피해자 PC에서 BSOD(Blue Screen Of Death)가 발생한다.

[피해자 PC BSOD 발생]

■ 취약점 상세 분석

Step 1. 동적 분석

BSOD 발생 시 생성된 crash dump[6]를 Windows용 디버깅 도구 WinDbg로 분석을 진행한다.

분석 결과를 보면 문제가 발생한 서비스는 HTTP 프로토콜 스택(http.sys)이며 UlFreeUnknownCodingList 함수의 LIST_ENTRY 구조체에 손상이 일어난 것을 알 수 있다.

```
25  PROCESS_NAME:  System
26
27  ERROR_CODE: (NTSTATUS) 0xc0000409 - The system detected an overrun of a stack-based buff
28
29  SYMBOL_NAME:  HTTP!UlFreeUnknownCodingList+63
30
31  MODULE_NAME: HTTP
32
33  IMAGE_NAME:  HTTP.sys
34
35  FAILURE_BUCKET_ID:  0x139_3_CORRUPT_LIST_ENTRY_HTTP!UlFreeUnknownCodingList
```

[LIST_ENTRY 손상]

LIST_ENTRY 구조체가 두 번 해제되었기 때문에 손상이 일어나, 그로 인해 BSOD가 발생하였음을 확인할 수 있다.

```
1  KERNEL_SECURITY_CHECK_FAILURE (139)
2  A kernel component has corrupted a critical data structure.  The corruption
3  could potentially allow a malicious user to gain control of this machine.
4  Arguments:
5  Arg1: 0000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).
6  Arg2: ffffa10287993480, Address of the trap frame for the exception that caused the bugcheck
7  Arg3: ffffa102879933d8, Address of the exception record for the exception that caused the bugcheck
8  Arg4: 0000000000000000, Reserved
```

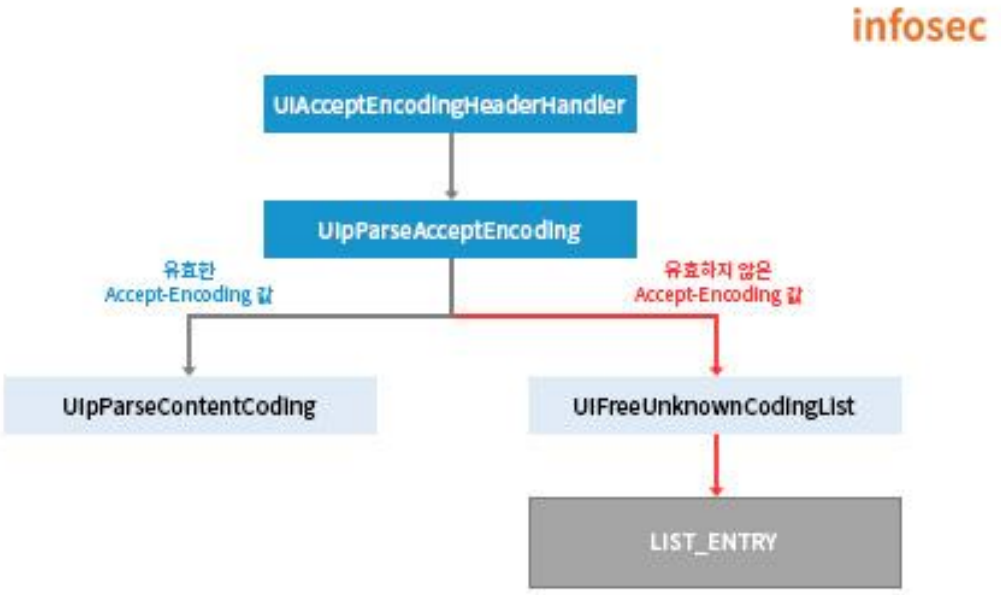
[KERNEL_SECURITY_CHECK_FAILURE(139)[7]]

6 crash dump 는 시스템 충돌이 발생 시 오류 원인 등의 내용을 하드 디스크에 기록한 덤프 파일이며, BSOD 관련 파일 생성 경로는 C:₩Windows₩MEMORY.DMP 이다.

7 해당 코드는 BSOD 가 발생하였을 때 생성되는 코드이다.

Step 2. Accept-Encoding

HTTP 요청을 받은 서버는 콘텐츠 협상[8] 과정을 거치며, UlAcceptEncodingHeaderHandler 함수를 호출하여, 클라이언트로부터 전달받은 Accept-Encoding 값을 쉼표를 기준으로 값에 대한 유효성 검사를 진행한다.



[Accept-Encoding 구문 분석 흐름도]

전달받은 값이 유효한 값일 경우 UlpParseContentCoding 함수를 호출하고, 유효하지 않은 값일 경우 UlFreeUnknownCodingList 함수를 호출하게 되는데, 해당 함수는 LIST_ENTRY 라는 구조체로 되어있다.

※ 윈도우 커널에서 대부분의 데이터 구조는 리스트 헤드에서 리스트 요소를 가리키는 링크 구조로 되어있다. 이때 LIST_ENTRY 구조체는 데이터들의 이중 순환 연결 리스트를 구현하기 위해 사용하는 구조체이다.

[8] 컨텐츠 협상이란 클라이언트가 특정 리소스를 요청할 경우 그에 맞는 형태의 리소스를 응답할 수 있도록 서버와 협상하는 과정이다.

Step 3. PoC 분석

이중 순환 연결을 위해 사용되는 LIST_ENTRY 구조체를 살펴보면, 이중 순환 연결을 위해 리스트의 이전 항목(Blink)과 다음 항목(Flink)에 대한 정보를 가지고 있다. Blink 와 Flink 모두 내용이 비어있거나, 이전 및 다음 항목에 대한 정보가 없는 경우 구조체의 헤더를 가리킨다.

```
typedef struct _LIST_ENTRY {
    struct _LIST_ENTRY *Flink;
    struct _LIST_ENTRY *Blink;
} LIST_ENTRY, *PLIST_ENTRY, PRLIST_ENTRY;
```

[LIST_ENTRY 구조체]

CVE-2022-21907 의 취약점을 유발하는 페이로드는 임의의 값이 나열되고, 마지막에 한 개의 빈 값과 한 개의 공백이 삽입된다. 앞서 살펴봤듯이 LIST_ENTRY 구조체는 값이 비어 있으면 구조체의 헤더를 가리키는데, 페이로드에서 두 개의 값이 비어 있기 때문에 같은 공간을 가리키게 된다. 그로 인해 충돌이 일어나, BSOD 가 발생하게 된다.

```
if __name__ == '__main__':
    options = parseArgs()

    if not options.target.startswith('http://') and not options.target.startswith('https://'):
        target = "http://" + options.target
    else:
        target = options.target

    payload = 'AAAAAAAAAAAAAAAAAAAAAAAA,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA&AA&
**AAAAAAAAAAAAAAAAAAAAA**A,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,AAAAAAAAAAAAAAAAAAAAAAAAAAA,
*****************************AAAAAA, *, ,'
```

[PoC 코드]

■ 대응 방안

2022년 1월 정기 패치를 통해 취약한 버전의 Windows 대한 보안 업데이트가 발표되었다.

infosec

KB 번호	Windows 버전	보안 업데이트 링크
KB5009557	Windows 10 Version 1809	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5009557
	Windows Server 2019	
KB5009543	Windows 10 Version 20H2	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5009543
	Windows 10 Version 21H1	
	Windows 10 Version 21H2	
KB5009566	Windows 11	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5009566
KB5009555	Windows Server 2022	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5009555

※ Windows 10 Version 1809, Windows Server 2019의 경우 기본적으로 취약하지 않은 버전이지만, HTTP 트레일러 지원이 활성화된 경우 취약하다. 따라서 아래 경로의 레지스트리 값 중 EnableTrailerSupport 값이 활성화되어 있다면 비활성화해야 한다.

HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩Services₩HTTP₩Parameters

※ EnableTrailerSupport 레지스트리 키는 Windows 10 Version 1809, Windows Server 2019에만 있다.

■ 참고 사이트

- URL : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907
- URL : https://github.com/nu11secur1ty/Windows10Exploits/tree/master/2022/CVE-2022-21907
- URL : https://github.com/p0dalirius/CVE-2022-21907-http.sys
- URL : https://developer.mozilla.org/ko/docs/Web/HTTP
- URL : https://www.zerodayinitiative.com/blog/2021/5/17/cve-2021-31166-a-wormable-code-execution-bug-in-httpsys

EQST INSIGHT

2022.02

SK쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST 담당
제　작 : SK쉴더스 PR팀