Research & Technique

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[1] 10점 만점 중 9.8점의 높은 점수를 받았다. 또한, 워머블(wormable)한 특성이 있어 네트워크를 통한 자가 전파가 가능하기 때문에 더욱 주의가 필요하다.

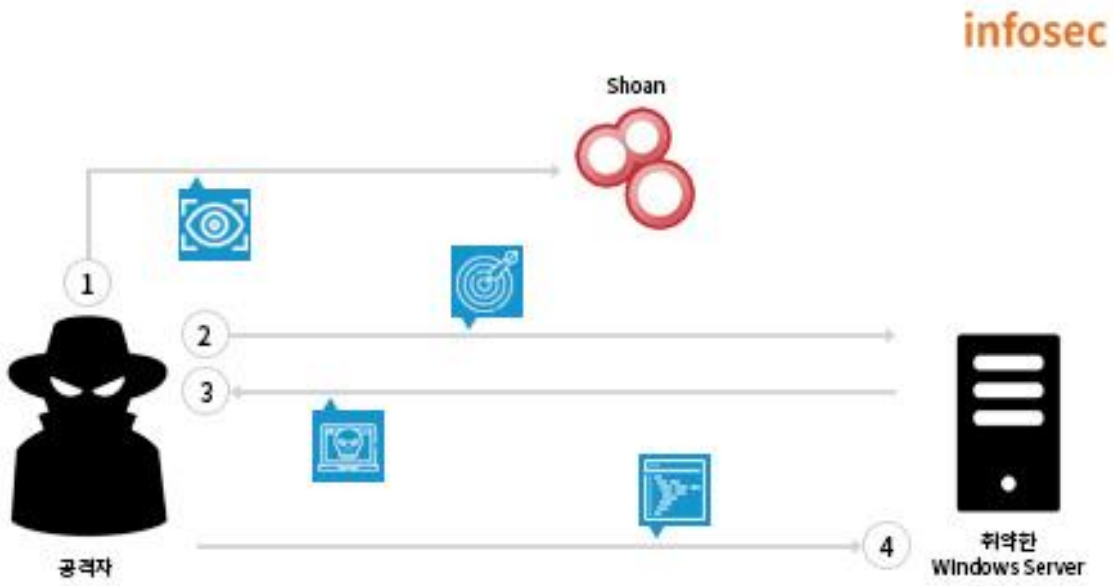
■ 영향 받는 소프트웨어 버전

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

[1] Common Vulnerability Scoring System으로 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

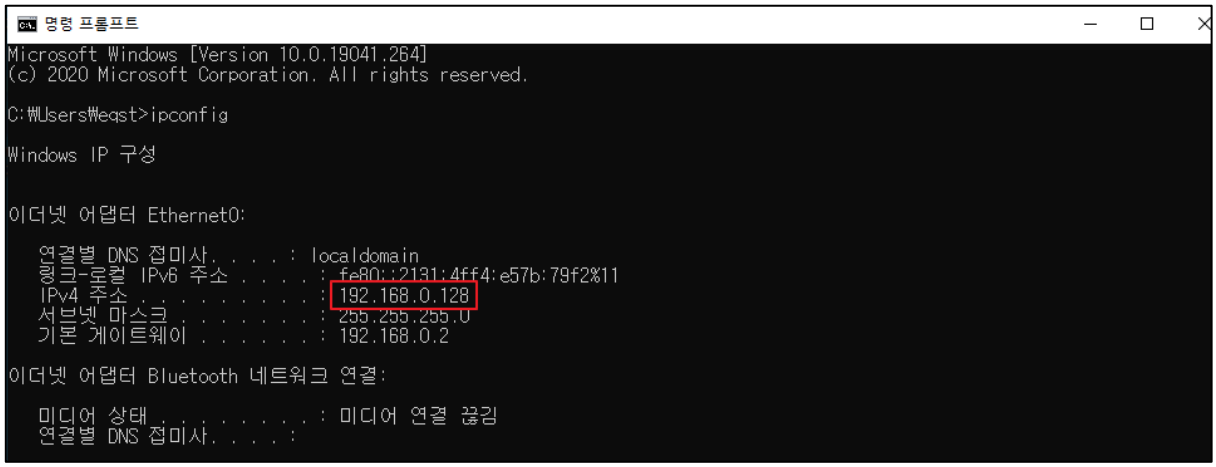
■ 취약점 테스트

Step 1. 환경구성

step 1) CVE-2022-21907은 HTTP 프로토콜 스택(http.sys)의 취약점으로 이를 사용하는 서비스[2]로 환경구성[3]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.

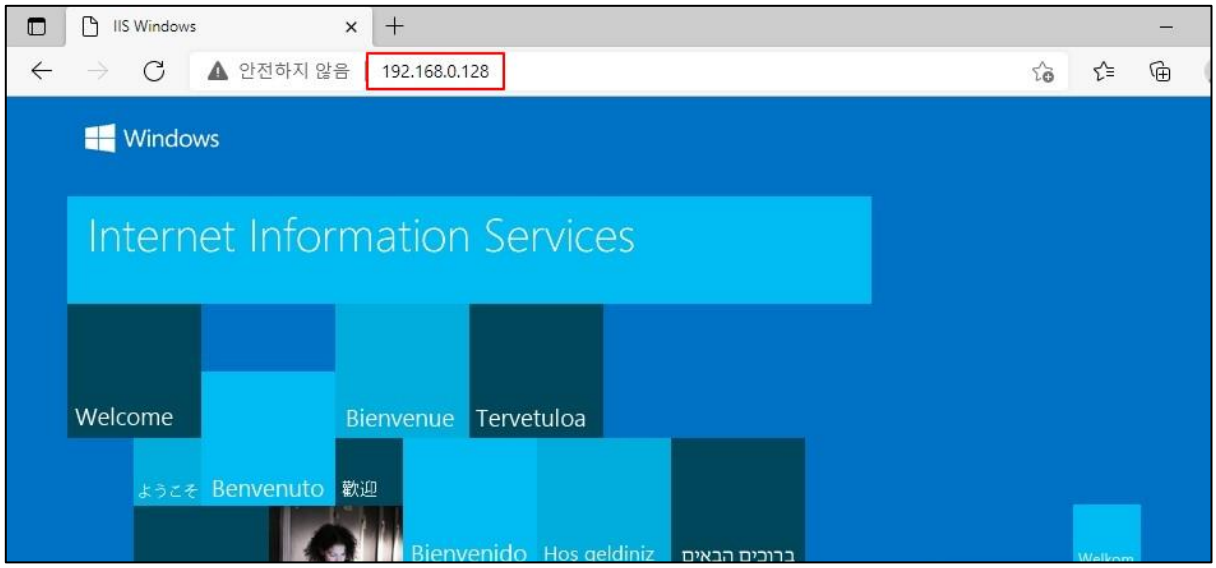


[피해자 IP 주소]

[2] http.sys를 사용하는 서비스에는 IIS 서버를 비롯해 WinRM, WSDAPI 등이 있다.

[3] 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]

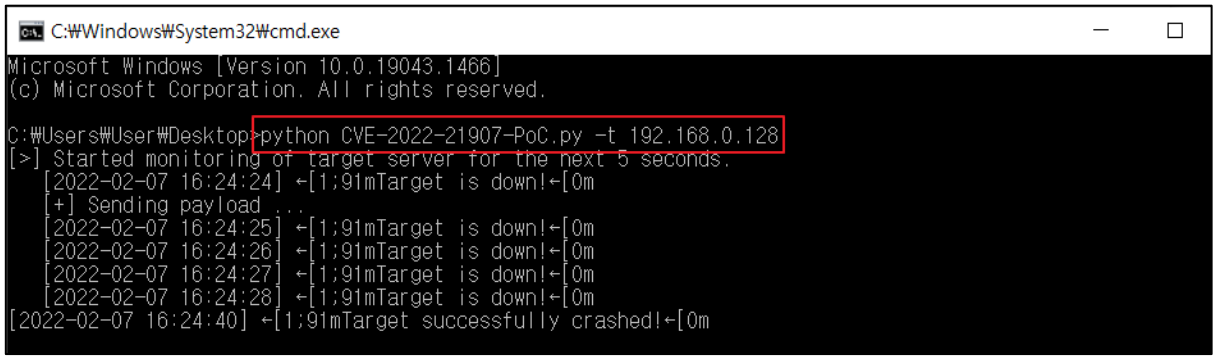
Step 2. PoC 테스트

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[4]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
```

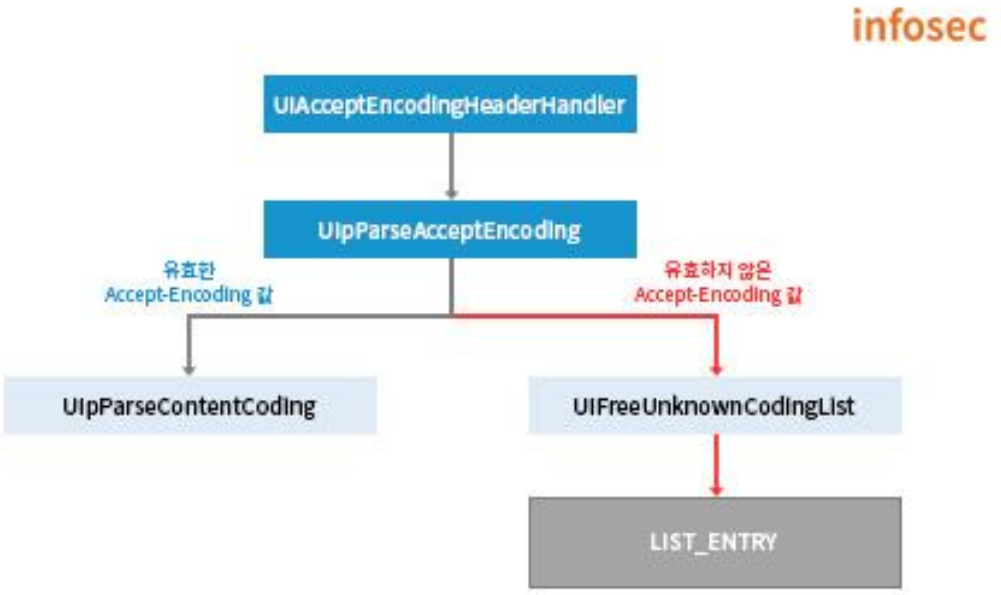
[KERNEL_SECURITY_CHECK_FAILURE(139)[5]]

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

[5] 해당 코드는 BSOD가 발생하였을 때 생성되는 코드이다.

Step 2. Accept-Encoding

HTTP 요청을 받은 서버는 콘텐츠 협상[6] 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.

[6] 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,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA&AA&
**AAAAAAAAAAAAAAAAAAAA**A,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,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