BOLETÍN DE ALERTA

Boletín Número: 2021-10 **Fecha de Publicación:** 10/09/2021
Tema: Nueva vulnerabilidad de 0-Day que afecta a Microsoft MSHTML en productos Office.

SEVERIDAD: ALTA

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de una nueva vulnerabilidad de ejecución de código remoto en Microsoft MSHTML en producto MS Office.

MSHTML es un motor de renderizado de navegador que permite que el navegador web Microsoft Internet Explorer lea y muestre páginas web HTML.

Los atacantes están abusando del documento de Microsoft Office al crear un control ActiveX malicioso que se aloja en el motor de procesamiento del navegador, y la vulnerabilidad se activará cuando las víctimas abran el documento malicioso de MS Office.

Microsoft asignó un CVE-2021-40444 para esta vulnerabilidad de ejecución remota de código MSHTML y la marcó como una vulnerabilidad de gravedad alta con un nivel de impacto de 8.8 / 10.

Recursos Afectados:

- Productos Office de Windows: 8.1, 10, 10 20H2, 10 21H1, 10 1507, 10 1511, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, 10 2004, RT 8.1
- Productos Office de Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2019 20H2, 2019 2004.

La vulnerabilidad de ejecución de código remoto en MSHTML que afecta a Microsoft Windows que consiste en ataques dirigidos que intentan aprovechar esta vulnerabilidad mediante el uso de documentos de Microsoft Office especialmente diseñados .

El atacante tendría que convencer al usuario de que abra el documento malicioso. Los usuarios cuyas cuentas están configuradas para tener menos derechos de usuario en el sistema podrían verse menos afectados que los usuarios que operan con derechos de usuario administrativos.

Microsoft MSHTML, también conocido como Trident, un motor patentado para internet Explorer y ahora descontinuado, que se usan en productos Microsoft Office para representar contenido web en interior por lo tanto la explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.

Además, el ataque se probó con éxito en la última versión de Office 2019 / Office 365 en Windows 10, y el ataque de día cero altamente sofisticado.

Poco después, el control ActiveX específico colocará el malware en el dispositivo de la víctima, que Microsoft llama ":" Ejecución sospechosa de archivo Cpl ".

Mitigación:

Una solución provisoria hasta que se publique un parche por parte del fabricante para esta vulnerabilidad de día 0, Microsoft recomendó deshabilitar la instalación de todos los controles ActiveX en Internet Explorer para mitigar este ataque.

Esto se puede lograr para todos los sitios mediante la actualización del registro. Los controles ActiveX instalados anteriormente seguirán ejecutándose, pero no exponen esta vulnerabilidad.

Cómo deshabilitar el control Activex:

1. Para deshabilitar la instalación de controles ActiveX en Internet Explorer en todas las zonas, pegue lo siguiente en un archivo de texto y guárdelo con la extensión de archivo .reg
2. Haga doble clic en el archivo .reg para aplicarlo a su sección de políticas.
3. Reinicie el sistema para asegurarse de que se aplique la nueva configuración.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Current
Version\Internet Settings\Zones\0]
"1001"=dword:00000003
"1004"=dword:00000003
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Current
Version\Internet Settings\Zones\1]
"1001"=dword:00000003
```

```
"1004"=dword:00000003
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Current Version\Internet Settings\Zones\2]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Current Version\Internet Settings\Zones\3]
"1001"=dword:00000003
"1004"=dword:00000003
-----------------------------------------------------------
```

Advertencia: Si usa el Editor del Registro incorrectamente, puede causar serios problemas que pueden requerir que reinstale su sistema operativo. Microsoft no garantiza que pueda resolver los problemas que resulten del uso incorrecto del Editor del Registro. Utilice el Editor del registro bajo su propia responsabilidad

Impacto de la solución alternativa.

Esto establece la URLACTION_DOWNLOAD_SIGNED_ACTIVEX (0x1001) y la URLACTION_DOWNLOAD_UNSIGNED_ACTIVEX (0x1004) en DISABLED (3) para todas las zonas de Internet para procesos de 64 y 32 bits. No se instalarán nuevos controles ActiveX. Los controles ActiveX instalados anteriormente seguirán ejecutándose.

¿Cómo deshacer la solución alternativa?

Elimine las claves de registro que se agregaron al implementar la solución.

Referencia:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
https://www.cert.gov.py/application/files/1016/3119/5601/BOL-CERT-PY-2021-20_Vulnerabilidad_de_ejecucion_de_codigo_remoto_en_Microsoft_MSHTML_en_productos_MS_Office.pdf
https://thehackernews.com/2021/09/new-0-day-attack-targeting-windows.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29
https://www.helpnetsecurity.com/2021/09/08/cve-2021-40444/