BOLETÍN DE ALERTA

Boletín Nro.: 2021-20

Fecha de publicación: 09/09/2021

Tema: Vulnerabilidad de ejecución de código remoto en Microsoft MSHTML en productos MS Office.

Fecha de actualización: 16/09/2021

Productos 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, 7.
- Productos Office de Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2019 20H2, 2019 2004.

Descripción:

Actores malintencionados se encuentran explotando la vulnerabilidad de ejecución de código remoto de Día Cero (Zero-Day) (CVE-2021-40444) en **Microsoft MSHTML** (también conocido como Trident), un motor de navegador patentado para Internet Explorer y ahora descontinuado, **que se usa en productos Microsoft Office** para representar contenido web en su interior.

La vulnerabilidad identificada como CVE-2021-40444 de severidad grave con una puntuación de 8.8, existe debido a una validación de entrada incorrecta dentro del componente MSHTML. **Un atacante remoto puede crear un documento de Office especialmente diseñado con un control ActiveX malicioso en su interior**, el atacante debe engañar a la víctima para que abra el documento y ejecutar el código arbitrario en el sistema. Los usuarios cuyas cuentas estén configuradas para tener menos derechos de usuario en el sistema podrían verse menos afectados que los usuarios que operan con derechos de usuario administrativo.

La vulnerabilidad se está explotando activamente en la naturaleza, pero no se conocen los detalles técnicos.

Impacto:

La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.

Solución:

Microsoft ha publicado actualizaciones de seguridad para abordar esta vulnerabilidad. Consulte la siguiente tabla de Actualizaciones de seguridad para conocer la actualización correspondiente a su sistema. Le recomendamos encarecidamente que instale estas actualizaciones inmediatamente.

Mitigación:

Microsoft Defender Antivirus y Microsoft Defender for Endpoint proporcionan detección y protección para la vulnerabilidad conocida. Los usuarios que utilizan actualizaciones automáticas no necesitan realizar ninguna acción adicional. Los usuarios empresariales que administran actualizaciones deben seleccionar la compilación de detección 1.349.22.0 o más reciente e implementarla en sus entornos. Las alertas de Microsoft Defender para Endpoint se mostrarán como: "Ejecución sospechosa de archivo Cpl". Sin embargo, es importante tener en cuenta que las organizaciones que solo ejecutan Microsoft Defender for Endpoint (no AV) no están protegidas de forma predeterminada. En ese caso, debe configurar EDR en modo de bloqueo.

Soluciones alternativas:

Hasta que se publique un parche por parte del fabricante, aconsejamos a los administradores deshabilitar ActiveX en Internet Explorer para mitigar el riesgo.

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.

Para deshabilitar los controles ActiveX en un sistema individual:

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

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\Internet Settings\Zones\0]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\Internet Settings\Zones\1]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Curre
ntVersion\Internet Settings\Zones\2]
"1001"=dword:00000003
"1004"=dword:00000003

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

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.

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.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
- https://www.helpnetsecurity.com/2021/09/08/cve-2021-40444/
- 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