CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad Zero-Day Microsoft Office

Fecha: 06/09/2022

Problemática: Zero-Day RCE en Microsoft Office (aka 'Follina')

Correlativo: AA-0019

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El equipo de investigadores en Ciberseguridad @Nao_Sec, descubrió un documento de Microsoft Office malicioso, que fue compartido en la plataforma de VirusTotal. Este documento utilizaba un método de infección inusual, pero conocido, el que además logró evadir la detección de Microsoft Defender y algunos Detección y Respuesta de Amenazas de Puntos Finales - EDR.

SITUACIÓN

Esta vulnerabilidad permite a un atacante la ejecución remota de código cuando se llama a MSDT (Microsoft Support Diagnostic Tool) mediante el protocolo URL desde una aplicación de llamada como Word. Un atacante que aproveche con éxito esta vulnerabilidad puede ejecutar código arbitrario con los privilegios de la aplicación que realiza la llamada. Luego, el atacante puede instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas en el contexto permitido por los derechos del usuario.

La vulnerabilidad se basa en un «nuevo» vector de ataque a través del protocolo «ms-msdt», que puede conducir a la ejecución remota de código sin necesidad de interacción por parte del usuario, ya que no involucra macros, e incluso, podría ser ejecutada desde la vista previa del documento ..

Los documentos en cuestión, utilizan la funcionalidad de plantilla remota para cargar el payload (HTML) desde una URL maliciosa, este archivo hace uso del handler «ms-msdt» para abrir Microsoft Support Diagnostics Tool (msdt.exe), herramienta legítima que permite ejecutar comandos a través de sus parámetros (tipo LOLBIN).

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Microsoft recomienda enfáticamente que los usuarios instalen las actualizaciones para estar completamente protegidos contra la vulnerabilidad.

1. Reforzar los protocolos de seguridad frente a documentos de Microsoft Office adjuntos en correos electrónicos sospechosos o no solicitados.
2. Mantener las plataformas de seguridad y sus reglas de detección al día.
3. En el caso de que un usuario abra un documento e inmediatamente se inicie la utilidad para «solucionar problemas de compatibilidad» se debe activar el protocolo de respuesta a incidentes.
4. Mantener activadas todas las configuraciones de seguridad en MS Office, especialmente la 'Vista protegida'.
5. Monitoreo y detección:
6. Se recomienda encarecidamente la supervisión de comportamientos sospechosos de los productos de Microsoft Office, por ejemplo, el proceso msdt.exe no debe ser generado desde productos de Office como words.exe, outlook.exe o excel.exe.

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

DICCIONARIO DE DATOS

1. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
2. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
3. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
4. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
5. IDS (Intrusion Detection System): Un sistema de detección de intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.
6. Virtual Private Network Red privada virtual (VPN): Tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.
7. Remote Desktop Protocol (RDP) (Protocolo de Escritorio Remoto): Protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.

REFERENCIAS

1. Documentación CVE-2022-30190 https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
2. https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug
3. https://attack.mitre.org/techniques/T1486/
4. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190
5. https://attack.mitre.org/techniques/T1566/
6. https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug

ÁREA PARA DEFINICIONES

La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.