Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Microsoft lanza parche para Follina

15/junio/2022

Contenido

INTRODUCCIÓN

Con este boletín queremos hacer de su conocimiento el reciente parche emitido por Microsoft para solventar la vulnerabilidad Follina, que permitía a los actores de amenazas atacar mediante documentos de Word para ejecutar comandos en PowerShell de forma oculta.

FOLLINA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_06_15_01
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	06/15/2022
Es día cero (0 day):	SI

RESUMEN

Microsoft emitió hoy un parche para la vulnerabilidad de día cero «Follina» divulgada recientemente y ampliamente explotada en la herramienta de diagnóstico de soporte de Microsoft (MSDT) como parte de su actualización de seguridad programada para junio.

El parche es uno de los más importantes de la 60 actualizaciones de seguridad que la compañía lanzó en total hoy para abordar las vulnerabilidades en su cartera de productos.

Microsoft evaluó la mayoría de las otras vulnerabilidades, incluidos muchos errores de ejecución remota de código, como «importantes».

Los productos afectados incluyeron Windows, Office, Edge, Visual Studio, Windows Defender, SharePoint Server y el Protocolo ligero de acceso a directorios de Windows.

Arreglo para la falla de Follina:

Los expertos en seguridad identificaron el parche para el Vulnerabilidad de Follina (CVE-2022-30190) como una prioridad debido a la forma activa en que se explota el error en la naturaleza. El error de MSDT, revelado el 30 de mayo, básicamente brinda a los atacantes una manera trivialmente fácil de ejecutar código de forma remota a través de documentos de Office. incluso cuando las macros están deshabilitadas. Microsoft advirtió sobre la vulnerabilidad que permite a los atacantes ver o eliminar datos, instalar programas y crear nuevas cuentas en sistemas comprometidos. Los ataques cibernéticos que explotan la falla se informaron al menos un mes antes del anuncio de Microsoft del 30 de mayo y desde entonces han crecido, impulsados por la disponibilidad pública del código de explotación.

La vulnerabilidad se puede explotar de manera trivial mediante un documento de Word especialmente diseñado que descarga y carga un archivo HTML malicioso a través de la función de plantilla remota de Word. El archivo HTML finalmente permite que el atacante cargue y ejecute el código de PowerShell dentro de Windows.

Johannes Ullrich, decano de investigación del Instituto SANS, dice que, por lo tanto, es una buena idea que las organizaciones mantengan Mitigaciones recomendadas por Microsoft para la falla en su lugar incluso después de instalar la actualización de MSDT. «Los usuarios que apliquen el paquete acumulativo mensual estarán protegidos, pero deben darse cuenta de que el parche solucionó la vulnerabilidad de inyección de código en msdt.exe. La herramienta de diagnóstico seguirá ejecutándose si un usuario abre un documento afectado.

El error de día cero se relaciona con una vulnerabilidad de ejecución remota de código que afecta a la Herramienta de diagnóstico de soporte de Windows (MSDT) cuando se invoca mediante el esquema de protocolo URI «ms-msdt:» desde una aplicación como Word.

«Un atacante que explota con éxito esta vulnerabilidad puede ejecutar código arbitrario con los privilegios de la aplicación que llama», dijo Microsoft en un aviso. «El atacante puede luego instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas en el contexto permitido por los derechos del usuario».

Un aspecto crucial de Follina es que explotar la falla no requiere el uso de macros, lo que elimina la necesidad de que un adversario engañe a las víctimas para que habiliten las macros para desencadenar el ataque.

Desde que surgieron los detalles del problema a fines del mes pasado, ha sido objeto de una amplia explotación por diferentes actores de amenazas para lanzar una variedad de cargas útiles como AsyncRAT, QBot y otros ladrones de información. La evidencia indica que Follina ha sido abusada en la naturaleza desde al menos el 12 de abril de 2022.

Recomendaciones

1. No descargar documentos que sean enviados por remitentes desconocidos, o documentos que usted no solicito.

2. Mantenga su software Antivirus actualizado.

3. Instalar los parches y actualizaciones de sistema que brinda Microsoft.

4. Solicitar a su SOC monitoreo sobre conexiones de red sospechosas a IP's con clasificación maliciosa.

5. Mantenga la autenticación de doble factor activa en todos los sistemas y dispositivos que permitan esta función.

Noticia Completa

https://teknomers.com/es/martes-de-parches-microsoft-soluciona-problemas-para-la-vulnerabilidad-follina-explotada-activamente/

https://cualesmi-ip.com/blog/microsoft-corrige-la-falla-de-dia-cero-follina-en-la-actualizacion-de-seguridad-mensual/

https://thehackernews.com/2022/06/patch-tuesday-microsoft-issues-fix-for.html

Enlace de descarga

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente