Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

LA VULNERABILIDAD CRÍTICA DE EJECUCIÓN DE CÓDIGO DE WINDOWS NO SE DETECTÓ HASTA AHORA

20 /Diciembre/2022

CONTENIDO

INTRODUCCIÓN 3

LA VULNERABILIDAD CRÍTICA DE EJECUCIÓN DE CÓDIGO DE WINDOWS NO SE DETECTÓ HASTA AHORA 4

RESUMEN 4

RECOMENDACIONES 6

NOTICIA COMPLETA 6

CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

Microsoft eleva la clasificación de seguridad para una vulnerabilidad similar a EternalBlue.

Los investigadores descubrieron recientemente una vulnerabilidad de ejecución de código de Windows que tiene el potencial de rivalizar con EternalBlue, el nombre de una falla de seguridad de Windows diferente utilizada para detonar WannaCry, el ransomware que cerró las redes informáticas en todo el mundo en 2017.

LA VULNERABILIDAD CRÍTICA DE EJECUCIÓN DE CÓDIGO DE WINDOWS NO SE DETECTÓ HASTA AHORA

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

ID de alerta:	DSOC-CERT_2022_12_20_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	20/12/2022
Es día cero (0 day):	Si

RESUMEN

Los investigadores descubrieron recientemente una vulnerabilidad de ejecución de código de Windows que tiene el potencial de rivalizar con EternalBlue, el nombre de una falla de seguridad de Windows diferente utilizada para detonar WannaCry, el ransomware que cerró las redes informáticas en todo el mundo en 2017.

Al igual que EternalBlue, CVE-2022-37958, como se rastrea la última vulnerabilidad, permite a los atacantes ejecutar código malicioso sin necesidad de autenticación. Además, al igual que EternalBlue, es gusano, lo que significa que un solo exploit puede desencadenar una reacción en cadena de exploits de seguimiento autorreplicantes en otros sistemas vulnerables. La capacidad de gusano de EternalBlue permitió que WannaCry y varios otros ataques se extendieran por todo el mundo en cuestión de minutos sin necesidad de interacción del usuario

Pero a diferencia de EternalBlue, que podría explotarse cuando se usa solo el SMB, o bloque de mensajes del servidor, un protocolo para compartir archivos e impresoras y actividades de red similares, esta última vulnerabilidad está presente en una gama mucho más amplia de protocolos de red, dando a los atacantes más flexibilidad de la que tenían al explotar la vulnerabilidad anterior.

Un factor potencialmente atenuante es que un parche para CVE-2022-37958 ha estado disponible durante tres meses. EternalBlue, por el contrario, fue explotado inicialmente por la NSA como un día cero. El exploit altamente armado de la NSA fue liberado en la naturaleza por un misterioso grupo que se hace llamar Shadow Brokers. La filtración, una de las peores en la historia de la NSA, dio a los hackers de todo el mundo acceso a un potente exploit de nivel de estado-nación.

RECOMENDACIONES

- Mantener al día las actualizaciones y parches de sus sistemas y servidores.
- Validar las conexiones SMB hacia sus equipos, hacer políticas fuertes en su Firewall para solo permitir las conexiones necesarias en sus servidores críticos.
- Instalar Sysmon en sus servidores para que se puedan monitorear las conexiones RDP y SMB directamente en los hosts.

NOTICIA COMPLETA

https://devel.group/blog/la-vulnerabilidad-critica-de-ejecucion-de-codigo-de-windows-no-se-detecto-hasta-ahora/

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