Investigadores de seguridad cibernética revelaron hoy una nueva vulnerabilidad crítica con una puntuación de gravedad de 10 sobre 10 en la escala CVSS, que afecta a las versiones de Windows Server 2003 a 2019.

La falla de ejecución remota de código de 17 años se rastrea como CVE-2020-1350, y se denominó SigRed por la compañía de seguridad cibernética Check Point.

Esta vulnerabilidad podría permitir que un atacante remoto no autenticado obtenga privilegios de administrador de dominio sobre los servidores seleccionados y tome el control completo de la infraestructura de TI de una organización.

Un actor de amenazas puede explotar la vulnerabilidad SigRed al enviar consultas DNS maliciosas creadas a un servidor DNS de Windows y lograr la ejecución de código arbitrario, lo que permite al hacker interceptar y manipular los correos electrónicos y el tráfico de red de los usuarios, hacer que los servicios no estén disponibles, entre otras acciones.

En un informe detallado compartido con Masterhacks, el investigador Sagi Tzadik, de Check Point, confirmó que la falla es de naturaleza *«wormable»*, lo que permite a los atacantes lanzar un ataque que puede propagarse de una computadora vulnerable a otra sin interacción humana.

> *«Un solo exploit puede iniciar una reacción en cadena que permita que los ataques se propaguen de una máquina vulnerable a otra sin requerir ninguna interacción humana. Esto significa que una sola máquina comprometida podría ser un 'super difusor', permitiendo que el ataque se extienda por toda la red de la organización a los pocos minutos del primer exploit»*, dijeron los investigadores.

Después de que la empresa de seguridad cibernética revelara sus hallazgos a Microsoft de forma responsable, el fabricante de Windows preparó un parche para la vulnerabilidad y lo implementó a partir de hoy como parte del martes de parches de julio, que también incluye actualizaciones de seguridad para otras 122 vulnerabilidades, con un total de 18 fallas en la

lista calificadas como críticas y otras 105 calificadas como importantes.

Microsoft aseguró no haber encontrado evidencia que demuestre que la vulnerabilidad ha sido explotada por los atacantes, pero aconsejó a los usuarios que instalen el parche de inmediato.

> *«Windows DNS Server es un componente central de la red. Aunque actualmente no se sabe que esta vulnerabilidad se use en ataques activos, es esencial que los clientes apliquen las actualizaciones de Windows para abordar la vulnerabilidad lo antes posible»,* dijo Microsoft.

Respuestas DNS maliciosas

Tomando como objetivo el identificar una vulnerabilidad que permitiría que un atacante no autenticado pusiera en peligro un entorno de dominio de Windows, los investigadores de Check Point aseguraron que se enfocaron en el DNS de Windows, específicamente observando de cerca cómo un servidor DNS analiza una consulta entrante o una respuesta para consulta reenviada.

Una consulta reenviada ocurre cuando un servidor DNS no puede resolver la dirección IP de un nombre de dominio determinado, lo que hace que la consulta se reenvíe a un servidor de nombres DNS autorizado.

Para la explotación de esta arquitectura, SigRed implica configurar los registros de recursos NS de un dominio («deadbeef.fun») para que apunten a un servidor de nombres malicioso («ns1.41414141.club»), y consultar el dominio del servidor DNS de destino para tener este último y analizar las respuestas del servidor de nombres para todas las consultas posteriores relacionadas con el dominio o subdominios.

Un atacante al contar con esta configuración, puede desencadenar una falla de

desbordamiento entero en la función que analiza las respuestas entrantes para las consultas reenviadas («dns.exe!SigWireRead») para enviar una respuesta DNS que contenga un registro de recursos SIG mayor de 64 KB e induzca un *«Desbordamiento de búfer basado en almacenamiento dinámico controlado de aproximadamente 64 KB sobre un búfer asignado pequeño».*

En otras palabras, la falla apunta a la función responsable de asignar memoria para el registro de recursos («RR_AllocateEx«), para generar un resultado mayor a 65535 bytes para causar un desbordamiento de enteros que conduce a una asignación mucho menor de lo esperado.

Pero con un solo mensaje DNS limitado a 512 bytes en UDP (o 4096 bytes si el servidor admite mecanismos de extensión) y 65535 bytes en TCP, los investigadores descubrieron que una respuesta SIG con una firma larga por sí sola no era suficiente para desencadenar la vulnerabilidad.

Para lograr esto, el ataque aprovecha la compresión del nombre DNS en las respuestas DNS para crear un desbordamiento del búfer utilizando la técnica mencionada antes, para aumentar el tamaño de la asignación en una cantidad significativa.

Explotación remota de la vulnerabilidad

Además, SigRed se puede activar remotamente por medio de un navegador en escenarios limitados, ya sea Internet Explorer y navegadores Microsoft Edge no basados en Chromium, lo que permite a un atacante abusar del soporte de los servidores DNS de Windows para la reutilización de conexiones y las características de canalización de consultas para obtener una consulta DNS dentro de una carga de solicitud HTTP a un servidor DNS de destino al visitar un sitio web bajo su control.

Por otro lado, el error puede explotarse más para filtrar direcciones de memoria al corromperlos metadatos de un registro de recursos DNS e incluso lograr capacidades de escritura, permitiendo que un adversario secuestre el flujo de ejecución y haga que ejecute

instrucciones no deseadas.

Algo que llama la atención es que los clientes DNS («dnsapi.dll»), no son susceptibles al mismo error, lo que lleva a los investigadores a sospechar que *«Microsoft administra dos bases de código completamente diferentes para el servidor DNS y el cliente DNS, y no sincroniza parches de errores entre ellos».*

Como solución temporal, la longitud máxima de un mensaje DNS sobre TCP se puede establecer en «0xF00» para eliminar las posibilidades de un desbordamiento del búfer:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Para
meters" /v "TcpReceivePacketSize" /t REG_DWORD /d 0xFF00 /f
```

```
net stop DNS && net start DNS
```

> *«Una violación del servidor DNS es algo muy serio. La mayoría de las veces, coloca al atacante a solo una pulgada de la violación de toda la organización. Solo hay un puñado de estos tipos de vulnerabilidad que se han lanzado»*, dijo el investigador Omri Herscovici.
>
> *«Todas las organizaciones, grandes o pequeñas que utilizan la infraestructura de Microsoft, corren un gran riesgo de seguridad si no se reparan. El riesgo sería una violación completa de toda la red corporativa»,* agregó.