Una investigación dejó al descubierto múltiples vulnerabilidades críticas de RDP inverso en Apache Guacamole, una popular aplicación de escritorio remoto utilizada por los administradores de sistemas para acceder y administrar máquinas Windows y Linux remotamente.

Los defectos informados podrían permitir que los atacantes logren tomar el control total sobre el servidor Guacamole, intercepten y controlen todas las demás sesiones conectadas.

Según el informe de Check Point Research, las fallas *«otorgan a un atacante, que ya ha comprometido con éxito una computadora dentro de la organización, lanzar un ataque contra la puerta de enlace de Guacamole cuando un trabajador desprevenido intenta conectarse a una máquina infectada».*

Después de que la empresa de seguridad cibernética revelara de forma responsable los hallazgos a Apache el 31 de marzo, los encargados del mantenimiento de Guacamole lanzaron una versión parcheada en junio de 2020.

Apache Guacamole es una popular solución de puertas de enlace de escritorio remoto sin cliente, de código abierto. Cuando se instala en el servidor de una empresa, permite a los usuarios conectarse de forma remota a sus escritorios simplemente utilizando un navegador web luego de un proceso de autenticación.

Particularmente, la aplicación de escritorio remoto Apache Guacamole, ha acumulado más de 10 millones de descargas hasta la fecha en Docker Hub.

Vulnerabilidad de corrupción de memoria

Los ataques derivan de una de las dos formas posibles en que la puerta de enlace puede ser tomada: ya sea por una máquina comprometida dentro de la red corporativa, que aprovecha una conexión benigna entrante para atacar la puerta de enlace de Apache, o un empleado deshonesto que utiliza una computadora dentro de la red para secuestrar la puerta.

El equipo de Check Point dijo que logró identificar las fallas como parte de la reciente auditoría de seguridad de Guacamole, que también agregó soporte para FreeRDP 2.0.0 a fines de enero de 2020.

Cabe mencionar que FreeRDP, un cliente RDP de código abierto, tenía su propia parte de los defectos de ejecución remota de código, que se revelaron a inicios del año pasado luego del lanzamiento de la versión 2.0.0-rc4.

> *«Siendo que las vulnerabilidades en FreeRDP solo fueron parcheadas en la versión 2.0.0-rc4, esto significa que todas las versiones que se lanzaron antes de enero de 2020 están usando versiones vulnerables de FreeRDP»*, dijo el investigador Eyal Itkin.

Estos son los defectos descubiertos:

- Vulnerabilidades de divulgación de información (CVE-2020-9497): Se identificaron dos fallas separadas en la implementación personalizada de los desarrolladores de un canal RDP utilizado para manejar paquetes de audio desde el servidor («rdpsnd»). El primer de los dos defectos permite a un hacker crear un mensaje rdpsnd malicioso, que podría conducir a una lectura fuera de límites similar a Heartbleed. El segundo error en el mismo canal, es una fuga de datos que transmite los datos fuera de los límites a un cliente conectado.

El tercer error de divulgación de información es una variante de la falla antes mencionada, que reside en un canal diferente llamado «guacai», responsable de la entrada de audio y está deshabilitado de forma predeterminada.

- Lecturas fuera de límites en FreeRDP: Al querer encontrar una vulnerabilidad de corrupción de memoria que pueda aprovecharse para explotar las fugas de datos anteriores, Check Point afirmó que descubrieron dos instancias adicionales de lecturas fuera de límites que aprovechan una falla de diseño en FreeRDP.

- Falla de corrupción de memoria en Guacamole (CVE-2020-9498): Esta falla está presente en la capa de abstracción («guac_common_svc.c»), colocada sobre los canales rdpsnd y rdpdr (redirección de dispositivo), surge de una violación de seguridad de la memoria, lo que resulta en una suspensión puntero que permite a un atacante lograr la ejecución del código al combinar ambos defectos.

Las vulnerabilidades sin uso son errores de corrupción de memoria que generalmente ocurren cuando una aplicación intenta utilizar el espacio de memoria que ya no está asignado. Esto, por lo general, hace que un programa se bloquee, pero también puede provocar otras consecuencias no deseadas, como la ejecución de código que puede ser explotada por actores maliciosos.

Con el uso de las vulnerabilidades CVE-2020-9497 y CVE-2020-9498, *«una computadora corporativa maliciosa (nuestro servidor RDP) puede tomar el control del proceso guacd cuando un usuario remoto solicita conectarse a su computadora»*, dijeron los investigadores.

Escalada de privilegios

Check Point descubrió que también era posible tomar el control de todas las conexiones en la puerta de enlace desde un solo proceso guacd, que se ejecuta en el servidor Guacamole para manejar conexiones remotas a la red corporativa.

Además de controlar la puerta de enlace, la escalada de privilegios permite a un atacante espiar todas las sesiones entrantes, registrar las credenciales utilizadas e incluso, comenzar nuevas sesiones para controlar el resto de las computadoras de la organización.

> *«Si bien la transición al trabajo remoto desde casa es una necesidad en estos tiempos difíciles de la pandemia de COVID-19, no podemos descuidar las implicaciones de seguridad de estas conexiones remotas»*, dijo Itkin.

> *«Recomendamos encarecidamente que todos se aseguren de que todos los servidores estén actualizados y que cualquier tecnología utilizada para trabajar desde casa esté completamente parcheada para bloquear los intentos de ataque»,* concluyó.