Los investigadores en ciberseguridad han revelado nuevas fallas de seguridad que afectan a Citrix Virtual Apps y Desktop, las cuales podrían ser aprovechadas para permitir la ejecución remota de código (RCE) sin autenticación.

El problema, de acuerdo con los hallazgos de watchTowr, está en el componente de grabación de sesiones, que permite a los administradores capturar la actividad de los usuarios, registrar las entradas del teclado y el ratón, así como grabar un video del escritorio con fines de auditoría, cumplimiento y diagnóstico.

Específicamente, la vulnerabilidad explota una *«combinación de una instancia de MSMQ expuesta negligentemente con permisos mal configurados que aprovechan BinaryFormatter y que puede ser accedida desde cualquier host mediante HTTP para realizar RCE sin autenticación»*, explicó el investigador de seguridad Sina Kheirkhah.

A continuación, se presentan los detalles de la vulnerabilidad:

- CVE-2024-8068 (Puntuación CVSS: 5.1) – Escalación de privilegios para obtener acceso a la cuenta NetworkService
- CVE-2024-8069 (Puntuación CVSS: 5.1) – Ejecución limitada de código remoto con privilegios de acceso a la cuenta NetworkService

Citrix, sin embargo, señaló que, para explotar la vulnerabilidad de manera exitosa, el atacante debe ser un usuario autenticado en el mismo dominio de Active Directory de Windows que el dominio del servidor de grabación de sesiones, y estar en la misma intranet que dicho servidor. Estas vulnerabilidades se han corregido en las siguientes versiones:

- Citrix Virtual Apps and Desktops antes del hotfix 24.5.200.8 de la versión 2407
- Citrix Virtual Apps and Desktops 1912 LTSR antes del hotfix 19.12.9100.6 del CU9
- Citrix Virtual Apps and Desktops 2203 LTSR antes del hotfix 22.03.5100.11 del CU5
- Citrix Virtual Apps and Desktops 2402 LTSR antes del hotfix 24.02.1200.16 del CU1

Es importante destacar que Microsoft ha recomendado a los desarrolladores dejar de utilizar

BinaryFormatter para la deserialización, ya que no es seguro cuando se usa con datos no confiables. La implementación de BinaryFormatter fue eliminada de .NET 9 a partir de agosto de 2024.

> *«BinaryFormatter se implementó antes de que las vulnerabilidades de deserialización fueran una categoría de amenaza bien comprendida. Como resultado, el código no sigue las mejores prácticas actuales. BinaryFormatter.Deserialize puede ser vulnerable a otras categorías de ataque, como la divulgación de información o la ejecución remota de código»,* menciona Microsoft en su documentación.

El núcleo del problema está en el Session Recording Storage Manager, un servicio de Windows que administra los archivos de las sesiones grabadas recibidos de cada computadora con esta función habilitada.

Mientras el Storage Manager recibe las grabaciones de sesión como bytes de mensaje a través del servicio Microsoft Message Queuing (MSMQ), el análisis mostró que se utiliza un proceso de serialización para transferir los datos y que la instancia de la cola tiene privilegios excesivos.

Para empeorar la situación, los datos recibidos de la cola se deserializan usando BinaryFormatter, permitiendo a un atacante aprovechar los permisos inseguros establecidos durante el proceso de inicialización para enviar mensajes MSMQ diseñados especialmente a través de HTTP en internet.

> *«Sabemos que existe una instancia de MSMQ con permisos incorrectamente configurados y que utiliza la conocida clase BinaryFormatter para realizar la deserialización. Lo 'mejor de todo' es que se puede acceder no solo localmente a través del puerto TCP de MSMQ, sino también desde cualquier otro host, mediante HTTP»,* indicó Kheirkhah, describiendo los pasos para crear un exploit.

> *«Esta combinación permite una ejecución remota de código sin autenticación»*, concluyó el investigador.