Un equipo de investigadores de ciberseguridad de la Universidad de New Haven lanzó un video que demuestra cómo las vulnerabilidad que la mayoría de los programadores subestiman podrían haber permitido a los piratas informáticos evadir la privacidad y la seguridad de su experiencia de realidad virtual y del mundo real.

Los investigadores Ibrahim Baggli, Peter Casey y Martin Vondrácek compartieron la información exclusiva con The Hacker News, aunque sus detalles técnicos aún no están disponibles públicamente. Las vulnerabilidades descubiertas residían en una aplicación popular de realidad virtual (VR) llamada Bigscreen Unity, una plataforma de desarrollo de videojuegos sobre la que se construye Bigscreen.

Bigscreen es una popular aplicación de realidad virtual que se describe a sí misma como una «*sala de estar virtual*», que permite a los amigos pasar el rato en un mundo virtual, ver películas, chatear, crear salas privadas, colaborar en proyectos, compartir experiencias, etc.

En el video se muestra que las fallas en la aplicación Bigscreen literalmente permitieron a los investigadores secuestrar de forma remota la infraestructura web de Bigscreen, que se ejecuta detrás de su aplicación de escritorio, y realizar múltiples escenarios de ataque por medio de un servidor de comando y control diseñado especialmente, que incluye:

- Descubrir habitaciones privadas
- Unirse a cualquier sala de realidad virtual, incluidas las habitaciones privadas
- Espiar a los usuarios mientras permanecen invisibles en cualquier sala de realidad virtual
- Ver las pantallas de las computadoras de los usuarios de VR en tiempo real
- Recibir sigilosamente el uso compartido de la pantalla de la víctima, el audio y el audio del micrófono
- Enviar mensajes en nombre del usuario
- Eliminar/prohibir a los usuarios de una habitación
- Configurar un gusano autorreplicante que podría extenderse por la comunidad de Bigscreen

Pero existe algo más preocupante, una vulnerabilidad diferente en la API de secuencias de comandos de Unity Engine que los investigadores explotaron en combinación con la falla de Bigscreen, que les permitió incluso tener un control completo sobre las computadoras de los usuarios de VR mediante la descarga e instalación secretas de malware o la ejecución de comandos maliciosos sin necesidad de interacción adicional.

Según los detalles técnicos, varias fallas de Bigscreen son problemas persistentes y almacenados de secuencias de comandos entre sitios (XSS), que residen en los campos de entrada donde los usuarios de VR deben enviar su nombre de usuario, nombre de sala, descripción de la habitación, categoría de habitación en la aplicación Bigscreen.

Investigadores muestran las vulnerabilidades de Biscreen VR

Dado que las casillas de entrada vulnerables no fueron saneadas, los atacantes podrían haber aprovechado la falla para inyectar código JavaScript malintencionado en la aplicación instalada por otros usuarios que se conectan al lobby de Bigscreen y a las salas de realidad virtual.

> *«El script de carga útil se ejecutará cuando el jugador basado en navegador ingrese a una sala que afecte a todos los miembros de la sala. Este vector de ataque permite la modificación/invocación de cualquier variante o función dentro del alcance de la ventana»,* dijeron los investigadores.
>
> *«En resumen, la capacidad de ejecutar JavaScript en la máquina de la víctima permite muchos otros ataques, como ventanas emergentes de suplantación de identidad, mensajes falsificados y uso compartido de escritorio forzado. Observamos una falta de autenticación al manejar la unión de salas privadas y las comunicaciones con el servidor de señalización Bigscreen. Como resultado, surgen varias vulnerabilidades potenciales, que incluyen la denegación de servicio, la manipulación de salas públicas, los ataques de fuerza bruta y el agotamiento de los*

> *recursos del servidor»,* agregaron.

Como lo demostró el equipo, los atacantes también pueden inyectar cargas de JavaScript maliciosas para aprovechar una API de scripts de Unity no documentada y potencialmente peligrosa para descargar en secreto malware de Internet y ejecutarlo en un sistema específico o para todos los usuarios.

> *«Se encontró que la función Unity.openLink () lanzaba enlaces web en los navegadores predeterminados 6. Un ataque XSS que contiene un enlace HTTP, FTP o SMB podría hacer que se buscaran y descargaran archivos arbitrarios»,* dijeron los investigadores.
>
> *«Esperamos que la mayoría de las aplicaciones que utilizan la API Unity afectada puedan ser vulnerables»,* agregaron.

El equipo descubrió las vulnerabilidades mientras probaba la seguridad de los sistemas de VR por medio de su proyecto financiado por la Fundación Nacional de Ciencia.

Man-in-the-Room es uno de los escenarios de ataque en los que un pirata informático se une en secreto a una sala de realidad virtual mientras permanece invisible para otros usuarios en la misma sala.

> *«No pueden verte, no pueden escucharte, pero el pirata informático puede escucharlos y verlos, como un Peeping Tom invisible. Una capa diferente de privacidad ha sido invalidada»*, dijo Ibrahim Baggili, fundador y codirector del Grupo de Investigación y Educación Ciber Forense.

El equipo descubrió que la aplicación Bigscreen utiliza bibliotecas cargadas dinámicamente

sin verificación de integridad que permitía a los investigadores modificar el código fuente de las bibliotecas seleccionadas y cambiar su comportamiento, lo que les permite ocultar su presencia de la interfaz de usuario utilizando las cargas útiles de XSS.

> «Nuestra aplicación WebRTC de prueba de concepto pudo conectarse a la aplicación Bigscreen legítima. Esto llevó al control completo sobre un *extremo de las secuencias de audio, video, micrófono y datos. Nuestra aplicación era invisible en la sala de realidad virtual porque no enviaba datos a otros peers*», dijeron.

El equipo informó responsablemente sus hallazgos tanto a Bigscreen como a Unity. Bigscreen reconoció las vulnerabilidades de seguridad en sus *«servidores y sistemas de transmisión»* y lanzó la nueva actualización 2019 de Bigscreen Beta que solucionó los problemas.

Además, Unity reconoció las vulnerabilidades simplemente agregando una nota a su documentación que indica que su plataforma *«se puede utilizar para abrir más que solo páginas web, por lo que tiene una importante implicación de seguridad que debe conocer».*