Google envió el lunes actualizaciones de seguridad para abordar una vulnerabilidad de día cero de alta gravedad en su navegador web Chrome, que según la compañía, está siendo explotada en la naturaleza.

La vulnerabilidad, rastreada como CVE-2022-2294, se relaciona con una falla de desbordamiento del montón en el componente WebRTC que brinda capacidades de comunicación de audio y video en tiempo real en los navegadores sin la necesidad de instalar complementos o descargar aplicaciones nativas.

Los desbordamientos de búfer de almacenamiento dinámico, también conocidos como desbordamiento de almacenamiento dinámico o destrucción de almacenamiento dinámico, ocurren cuando los datos se sobrescriben en el área de almacenamiento dinámico de la memoria, lo que lleva a la ejecución de código arbitrario o a una condición de denegación de servicio (DoS).

> *«Los desbordamientos basados en montón se pueden usar para sobrescribir punteros de función que pueden estar viviendo en la memoria, apuntándolos al código del atacante. Cuando la consecuencia es la ejecución de código arbitrario, esto por lo general se puede usar para subvertir cualquier otro servicio de seguridad»*, explicó MITRE.

Fue acreditado por informar la vulnerabilidad el 1 de julio de 2022, Jan Vojtesek del equipo de Avast Threat Intelligence. Cabe mencionar que el error también afecta la versión de Chrome para Android.

Como pasa con la explotación de Día Cero, los detalles relacionados con la vulnerabilidad y otros detalles específicos relacionados con la campaña se han retenido para evitar más abusos en la naturaleza y hasta que una parte significativa de los usuarios se actualicen con una solución.

CVE-2022-2294 también marca la resolución de la cuarta vulnerabilidad de día cero en

Chrome desde inicio de año:

- CVE-2022-0609: Use-after-free en Animación
- CVE-2022-1096: Confusión de tipo en V8
- CVE-2022-1364: Confusión de tipo en V8

Se recomienda a los usuarios actualizar a la versión 103.0.5060.114 para Windows, macOS y Linux y 103.0.5060.71 para Android para mitigar posibles amenazas.

También se recomienda a los usuarios de navegadores basados en Chromium como Microsoft Edge, Brave, Opera y Vivaldi que apliquen las correcciones cuando estén disponibles.

La divulgación sigue poco después de un informe de Google Project Zero, que señaló que un total de 18 vulnerabilidades de seguridad se han explotado como días cero sin parches en lo que va del año.