El navegador web Google Chrome para Windows, Mac o Linux, tiene problemas graves de seguridad, por lo que es importante actualizar a la última versión lanzada este jueves lo más pronto posible.

Google lanzó la versión 86.0.4240.111 de Chrome para corregir varios problemas de seguridad de alta gravedad, incluida una vulnerabilidad de día cero que los hackers explotaron en la naturaleza para secuestrar computadoras específicas.

Rastreada como CVE-2020-15999, la vulnerabilidad explotada activamente es un tipo de falla de corrupción de memoria, llamada desbordamiento de búfer de pila en Freetype, una popular biblioteca de desarrollo de software de código abierto para renderizar fuentes, que viene empaquetada con Chrome.

La vulnerabilidad fue descubierta e informada por el investigador de seguridad cibernética, Sergei Glazunov, de Google Project Zero, el 19 de octubre y está sujeta a un plazo de divulgación pública de siete días debido a que la falla se encuentra bajo explotación activa.

Glazunov también informó inmediatamente de la vulnerabilidad de día cero a los desarrolladores de Freetype, quienes desarrollaron un parche de emergencia para abordar el problema el pasado 20 de octubre, con el lanzamiento de FreeType 2.10.4.

Aunque no se revelaron detalles técnicos de la vulnerabilidad, el líder técnico de Google Project Zero, Ben Hawkes, advirtió en Twitter que aunque el equipo solo ha detectado un exploit dirigido a los usuarios de Chrome, es posible que otros proyectos que usan FreeType también sean vulnerables y se recomienda implementar la corrección de la última versión de FreeType.

> *«Si bien solo vimos un exploit para Chrome, otros usuarios de FreeType deberían adoptar la solución que se describe aquí: https://savannah.nongnu.org/bugs/?59308*

> *– la solución también se encuentra en la versión estable de FreeType 2.10.4 de hoy»*, dijo Hawkes.

Según los detalles compartidos por Glazunov, la vulnerabilidad existe en la función *«Load_SBit_Png»* de FreeType, que procesa imágenes PNG incrustadas en fuentes. Los atacantes pueden aprovecharlo para ejecutar código arbitrario simplemente al utilizar fuentes diseñadas específicamente con imágenes PNG incrustadas.

> *«El problema es que libpng utiliza los valores originales de 32 bits, que se guardan en 'png_struct'. Por lo tanto, si el ancho y/o alto originales son mayores que 65535, el búfer asignado no podrá ajustarse al mapa de bits»*, explicó Glazunov.

Google lanzó Chrome 86.0.4240.111 como la versión estable de Chrome, disponible para todos los usuarios, no solo para los usuarios beta, y dijo que la compañía está al tanto de los informes de que *«existe un exploit para CVE-2020-15999 en la naturaleza»*, pero no reveló más detalles sobre los ataques activos.

Además de la vulnerabilidad de día cero de FreeType, Google también corrigió cuatro fallas en la última actualización de Chrome, tres de las cuales son vulnerabilidades de alto riesgo: un error de implementación inapropiado en Blink, un problema después de un error libre en los medios de Chrome y un problema después de un error libre en PDFium, y otro problema de riesgo medio luego de una edición libre en la función de impresión del navegador.

Aunque Chrome notifica de forma automática a los usuarios cuando existen actualizaciones disponibles, se recomienda activar manualmente el proceso de actualización.