Google lanzó una actualización de software urgente para su navegador web Chrome, y pide a los usuarios de Windows, Mac y Linux que actualicen inmediatamente.

La versión de Chrome 77.0.3865.90 comenzó a implementarse para los usuarios de todo el mundo este miércoles, contiene parches de seguridad para una vulnerabilidad crítica y tres de alto riesgo, la más grave de estas, permitiría a los hackers remotos tomar el control de un sistema afectado.

Google decidió mantener en secreto los detalles de las cuatro vulnerabilidades por unos días más, con el fin de evitar que los hackers las exploten y brindar a los usuarios el tiempo suficiente para instalar la actualización de Chrome.

Mientras tanto, el equipo de seguridad de Chrome solo reveló que las cuatro vulnerabilidades son problemas sin uso en diferentes componentes del navegador web, como se menciona en la siguiente lista, que podrían provocar ataque de ejecución remota de código.

La vulnerabilidad de uso posterior libre es una clase de problema de corrupción de memoria, que permite la modificación de datos en memoria, permitiendo a un usuario sin privilegios escalar los mismos en un sistema o software afectado.

Vulnerabilidades parcheadas en Chrome 77.0.3865.90

- Use-after-free en UI (CVE-2019-13685), reportada por Khalil Zhani
- Use-after-free en los medios (CVE-2019-13688), reportada por Man Yue Mo, del Equipo de Investigación de Seguridad Semmle
- Use-after-free en los medios (CVE-2019-13687), reportada por Man Ye Mo, del Semmle
- Use-after-free en páginas offline (CVE-2019-13686), reportada por Brendon Tiszka.

Google pagó un total de 40,000 dólares en recompensas a Man Yue Mo de Semmle por las vulnerabilidades, 20 mil dólares por cada una, mientras que las recompensas por las dos vulnerabilidades restantes no se han establecido.

La explotación exitosa de estas vulnerabilidades podría permitir que un atacante ejecute código arbitrario en el contexto del navegador con solo convencer a las víctimas de que solo abran o redirijan a una página web específicamente diseñada en el navegador Chrome afectado, sin requerir interacciones adicionales.

Según divulgaciones anteriores, la falla de uso libre posterior también podría conducir a la divulgación de información confidencial, eludir las restricciones de seguridad, acciones no autorizadas y causar condiciones de denegación de servicio, dependiendo de los privilegios asociados con la aplicación.

Aunque Google Chrome notifica de forma automática a los usuarios sobre la última versión disponible del software, se recomienda a los usuarios activar manualmente el proceso de actualización en Ayuda > Acerca de Google Chrome en el menú.