Investigadores de seguridad cibernética revelaron este lunes los detalles de una vulnerabilidad de día cero en los navegadores web basados en Chromium para Windows, Mac y Android, que podría haber permitido a los atacantes eludir completamente las reglas de la Política de Seguridad de Contenido (CSP) desde Chrome 73.

La vulnerabilidad rastreada como CVE-2020-6519, calificada con 6.5 en la escala CVSS, surge de una omisión de CSP que da como resultado la ejecución arbitraria de código malicioso en los sitios web de destino.

Según PerimeterX, algunos de los sitios web más populares, incluidos Facebook, Wells Fargo, Zoom, Gmail, WhatsApp, Investopedia, ESPN, Roblox, Indeed, TikTok, Instagram, Blogger y Quora, eran susceptibles a la omisión de CSP.

Algo que ha causado polémica es que Tencent Security Xuanu Lab, también informó sobre la misma falla hace mas de un año, un mes después del lanzamiento de Chrome 73 en marzo de 2019, pero nunca se abordó hasta que PerimeterX informó el problema a inicios de marzo.

Después de revelar los hallazgos a Google, el equipo de Chrome emitió una solución para la vulnerabilidad en la actualización de Chrome 84 (versión 84.0.4147.89), que comenzó a implementarse el 14 de julio.

CSP es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross-Site Scripting (XSS) y ataques de inyección de datos.

Con las reglas de CSP, un sitio web puede exigir al navegador de la víctima que realice ciertas verificaciones del lado del cliente con el objetivo de bloquear scripts específicos que están diseñados para explotar la confianza del navegador en el contenido recibido del servidor.

Debido a que CSP es el método principal utilizado por los propietarios de sitios web para hacer cumplir las políticas de seguridad de datos y evitar la ejecución de scripts maliciosos, una omisión de CSP puede poner en riesgo los datos del usuario de forma efectiva.

Esto se logra especificando los dominios que el navegador debe considerar como fuentes válidas de scripts ejecutables, de modo que un navegador compatible con CSP solo ejecute scripts cargados en archivos de origen recibidos de esos dominios permitidos, ignorando todos los demás.

La falla descubierta por Tencent y PerimeterX elude el CSP configurado para un sitio web simplemente pasando un código JavaScript malicioso en la propiedad «src» de un elemento iframe HTML.

Cabe mencionar que sitios como Twitter, Github, LinkedIn, Google Play Store, la página de inicio de Yahoo, PayPal y Yandex no se encontraron vulnerables debido a que las políticas de CSP se implementaron usando un nonce o hash para permitir la ejecución de scripts en línea.

> *«Tener una vulnerabilidad en el mecanismo de ejecución de CSP de Chrome no significa directamente que los sitios sean violados, ya que los atacantes también deben administrar para obtener el script malicioso llamado desde el sitio (por lo que la vulnerabilidad se clasificó como de gravedad media)»*, dijo Gal Weizman, de PerimeterX.

Aunque no se conocen las implicaciones de la vulnerabilidad, los usuarios deben actualizar sus navegadores a la última versión para protegerse contra la ejecución de dicho código. En el caso de los webmasters, es recomendable que utilicen las capacidades nonce y hash de CSP para mayor seguridad.

Aparte de este error, la última actualización de Chrome 84.0.4147.125 para sistemas Windows, Mac y Linux, también corrige otras 15 vulnerabilidades de seguridad, de las cuales, 12 están calificadas como altas y dos como bajas.