Investigadores de seguridad cibernética de Google brindaron más detalles este miércoles sobre cuatro vulnerabilidades de día cero en la naturaleza en los navegadores Chrome, Safari e Internet Explorer, que han sido explotadas por hackers en distintas campañas desde el comienzo del año.

Además, tres de los cuatro días cero fueron diseñados por proveedores comerciales y vendidos y utilizados por actores respaldados por el gobierno, lo que contribuyó a un aumento en los ataques del mundo real. La lista de vulnerabilidades ya parcheadas es:

- CVE-2021-1879: Use-After-Free en QuickTimePluginReplacement (Apple WebKit)
- CVE-2021-21166: Problema del ciclo de vida de los objetos de Chrome en audio
- CVE-2021-30551: Confusión de tipos de Chrome en V8
- CVE-2021-33742: Escritura fuera de límites de Internet Explorer en MSHTML

Se cree que los días cero de Chrome, CVE-2021-21166 y CVE-2021-30551, fueron utilizados por el mismo actor y se entregaron como enlaces únicos enviados por correo electrónico a los objetivos ubicados en Armenia, con los enlaces redirigidos a los usuarios desprevenidos que apuntan a dominios controlados por atacantes que se hacían pasar por sitios web legítimos de interés para los destinatarios.

Los sitios web maliciosos se encargaron de tomar las huellas digitales de los dispositivos, incluyendo la recopilación de información del sistema sobre los clientes, antes de entregar una carga útil de segunda etapa.

Cuando Google lanzó un parche para CVE-2021-30551, Shane Huntley, director del Grupo de Análisis de Amenazas (TAG) de Google, reveló que la vulnerabilidad fue aprovechada por el mismo actor que abusó de CVE-2021-33742, una ejecución remota de código explotada activamente en la plataforma Windows MSHTML que fue abordado por Microsoft como parte de su actualización del martes de parches del 8 de julio.

Las vulnerabilidades fueron proporcionadas por un corredor de explotación comercial a un adversario de un estado-nación, que los utilizó en ataques limitados contra objetivos en

Europa del Este y Medio Oriente, agregó Huntley.

Ahora, según un informe técnico publicado por el equipo, las tres vulnerabilidades fueron *«desarrollados por la misma empresa de videovigilancia comercial que vendió estas capacidades a dos actores diferentes respaldados por el gobierno».*

Agregó también que la vulnerabilidad de Internet Explorer se utilizó en una campaña de orientación con usuarios armenios mediante documentos de Office maliciosos que cargaron contenido web en el navegador.

Google no reveló las identidades del broker de exploits ni de los dos actores de amenazas que utilizaron las vulnerabilidades como parte de sus ataques.

Por otro lado, el día cero de Safari, se refería a una falla de WebKit que podría permitir a los adversarios procesar contenido web creado con fines malintencionados que puede resultar en ataques universales de scripts entre sitios. Apple corrigió el problema el 26 de marzo de 2021.