Google ha implementado medidas para impedir la aparición de anuncios en sitios de comercio electrónico que utilizan el servicio Polyfill.io después de que una compañía china adquiriera el dominio y modificara la biblioteca JavaScript («polyfill.js») para dirigir a los usuarios hacia sitios maliciosos y fraudulentos.

Más de 110,000 sitios que incorporan esta biblioteca se ven afectados por este ataque a la cadena de suministro, según reportó Sansec el martes.

Polyfill es una biblioteca popular que brinda soporte para funciones modernas en los navegadores web. A principios de febrero, surgieron preocupaciones después de que fuera adquirida por la empresa china Funnull, que gestiona una red de entrega de contenido (CDN).

Andrew Betts, el creador original del proyecto, instó a los propietarios de sitios web a eliminarla de inmediato, señalando que *«ningún sitio web en la actualidad requiere de los polyfills de la biblioteca polyfill[.]io»* y que *«la mayoría de las características agregadas a la plataforma web son adoptadas rápidamente por todos los navegadores principales, con algunas excepciones que generalmente no se pueden polifillar, como Web Serial y Web Bluetooth».*

Este desarrollo también llevó a los proveedores de infraestructura web Cloudflare y Fastly a ofrecer puntos finales alternativos para ayudar a los usuarios a alejarse de polyfill[.]io.

> *«Las preocupaciones radican en que cualquier sitio web que incluya un enlace al dominio original polyfill[.]io dependerá ahora de Funnull para mantener y proteger el proyecto subyacente, evitando así el riesgo de un ataque a la cadena de suministro»*, indicaron los investigadores de Cloudflare, Sven Sauleau y Michael Tremante.
>
> *«Este tipo de ataque podría ocurrir si el tercero subyacente resulta comprometido o altera el código que se sirve a los usuarios finales de manera maliciosa, provocando que todos los sitios web que utilizan la herramienta sean comprometidos».*

La empresa de seguridad en comercio electrónico con sede en los Países Bajos informó que el dominio «cdn.polyfill[.]io» ha sido detectado inyectando malware que redirige a los usuarios a sitios de apuestas deportivas y pornográficos.

> *«El código cuenta con medidas específicas para evitar la ingeniería inversa y solo se activa en dispositivos móviles particulares durante horas concretas. Tampoco se activa cuando detecta un usuario administrador. Además, retrasa la ejecución cuando detecta un servicio de análisis web, presumiblemente para evitar ser registrado en las estadísticas»,* detallaron.

La compañía con sede en San Francisco, c/side, también emitió una alerta propia, señalando que los administradores del dominio añadieron un encabezado de Protección de Seguridad de Cloudflare a su sitio entre el 7 y 8 de marzo de 2024.

Los hallazgos siguen a una advertencia sobre una vulnerabilidad crítica que afecta a los sitios web de Adobe Commerce y Magento (CVE-2024-34102, puntuación CVSS: 9.8) que sigue en gran parte sin parchear a pesar de que las correcciones están disponibles desde el 11 de junio de 2024.

> *«En sí misma, esta vulnerabilidad permite a cualquier persona leer archivos privados (como aquellos con contraseñas). Sin embargo, combinada con el reciente problema de iconv en Linux, se convierte en un grave problema de seguridad que facilita la ejecución de código remoto»,* dijo Sansec, que denominó la cadena de explotación CosmicSting.

Se ha revelado que terceros pueden obtener acceso administrativo API sin necesidad de una versión vulnerable de Linux al problema de iconv (CVE-2024-2961), lo que agrava aún más la situación.