Un investigador de seguridad descubrió una grave vulnerabilidad en la famosa plataforma de código abierto basada en eventos, StackStorm, que podría permitir a los atacantes remotos engañar a los desarrolladores para que ejecuten, sin saberlo, comandos arbitrarios en servicios específicos.

StackStorm, también conocida como *«IFTTT for Ops»*, es una poderosa herramienta de automatización dirigida por eventos para la integración y automatización de servicios y herramientas que permiten a los desarrolladores configurar acciones, flujos de trabajo y tareas programas, para realizar operaciones en servidores a gran escala.

Como ejemplo, se configurar instrucciones en la plataforma StackStorm para cargar de forma automática los paquetes de red en un servicio de análisis de redes basado en la nube, en eventos en los que el software de seguridad detecte una intrusión o actividad maliciosa en la red.

Debido a que StackStorm ejecuta acciones, que pueden ir desde solicitudes HTTP hasta comandos arbitrarios, en servidores o servicios remotos que los desarrolladores integran para tareas automatizadas, la plataforma se ejecuta con privilegios muy altos.

Barak Tawily, investigador de seguridad de aplicaciones, detalló que la falla residía en la forma en que la API REST de StackStorm manejaba de forma incorrecta los encabezados CORS, lo que a su vez permitió que los navegadores web enviaran solicitudes de dominio cruzado en nombre de los usuarios o desarrolladores autenticados en la interfaz de usuario.

> *«Específicamente, lo que la API de StackStorm devolvió para Access-Control-Allow-Origin, antes de StackStorm 2.10.3/2.9.3, si el origen de la solicitud era desconocido, era un valor nulo»,* dijo StackStorm.
>
> *«Como mostrará la documentación de Mozilla, se realizará una copia de seguridad del comportamiento del cliente, que puede resultar nulo en una solicitud exitosa de origen desconocido en algunos clientes, permitiendo la posibilidad de ataques de*

> *estilo XSS contra la API de StackStorm»*, agregó.

El encabezado Access-Control-Allow-Origin es fundamental para la seguridad de los recursos, ya que especifica qué dominios pueden acceder a los recursos de un sitio, que si se configuran de forma incorrecta en un sitio, podrían permitir que otros sitios malintencionados accedan a sus recursos de forma cruzada.

Para aprovechar la vulnerabilidad (CVE-2019-9580), un atacante simplemente necesita enviar un enlace malintencionado a una víctima, lo que le permite *«leer / actualizar / crear acciones y flujos de trabajo, obtener direcciones IP internas y ejecutar un comando en cada máquina que es accesible por el agente StackStorm».*

Tawily compartió un video de prueba de concepto con The Hacker News, que demuestra cómo la vulnerabilidad en StackStorm podría permitir a un atacante hacerse cargo de cualquier servidor accesible por el agente de StackStorm.

El investigador compartió sus hallazgos con el equipo de StackStorm la semana pasada, que reconoció el problema y lanzó inmediatamente las versiones 2.9.3 y 2.10.3 de StackStorm para abordar la vulnerabilidad. Se recomienda a los desarrolladores actualizar sus versiones.