Investigadores en ciberseguridad han expuesto múltiples fallos críticos de seguridad en la herramienta TorchServe, utilizada para servir y escalar modelos PyTorch, que podrían ser aprovechados en secuencia para lograr la ejecución remota de código en sistemas afectados.

La compañía de seguridad de aplicaciones en tiempo de ejecución con sede en Israel, Oligo, que hizo este descubrimiento, ha bautizado a estas vulnerabilidades como ShellTorch.

> *«Estas vulnerabilidades pueden desencadenar una Ejecución de Código Remoto (RCE) en cadena completa, dejando a miles de servicios y usuarios, incluyendo algunas de las empresas más grandes del mundo, vulnerables a accesos no autorizados e inserción de modelos de IA maliciosos, y potencialmente a una toma completa del servidor»,* afirmaron los investigadores de seguridad Idan Levcovich, Guy Kaplan y Gal Elbaz.

La lista de defectos, que han sido abordados en la versión 0.8.2, es la siguiente:

- Sin CVE – Configuración incorrecta de la API de la Interfaz de Gestión No Autenticada (0.0.0.0)
- CVE-2023-43654 (puntuación CVSS: 7.2) – Un fallo de solicitud forjada remota en el servidor que conduce a la ejecución remota de código.
- CVE-2022-1471 (puntuación CVSS: 9.9) – Uso de una versión insegura de la biblioteca de código abierto SnakeYAML, lo que permite la deserialización no segura de objetos Java.

La explotación exitosa de las fallas mencionadas anteriormente podría permitir que un atacante envíe una solicitud para cargar un modelo malicioso desde una dirección controlada por un actor, lo que llevaría a la ejecución de código arbitrario.

En otras palabras, un atacante que pueda acceder de forma remota al servidor de gestión también puede cargar un modelo malicioso, lo que permite la ejecución de código sin necesidad de autenticación en ningún servidor TorchServe predeterminado.

Aún más alarmante, estas debilidades podrían combinarse con CVE-2022-1471 para allanar el camino hacia la ejecución de código y la toma completa de las instancias expuestas.

> *«Los modelos de IA pueden incorporar un archivo YAML para definir su configuración deseada, por lo tanto, al cargar un modelo con un archivo YAML manipulado maliciosamente, logramos desencadenar un ataque de deserialización insegura que resultó en la ejecución de código en la máquina»,* informaron los investigadores.

La gravedad de estos problemas ha llevado a Amazon Web Services (AWS) a emitir una advertencia instando a los clientes que utilicen las versiones 1.13.1, 2.0.0 o 2.0.1 de los Contenedores de Aprendizaje Profundo (DLC) de PyTorch en EC2, EKS o ECS lanzados antes del 11 de septiembre de 2023 a actualizar a la versión 0.8.2 de TorchServe.

> *«Mediante el aprovechamiento de los privilegios otorgados por estas vulnerabilidades, es posible visualizar, alterar, apoderarse y eliminar modelos de IA y datos confidenciales que fluyen hacia y desde el servidor TorchServe de destino»*, destacaron los investigadores.

> *«Aún más alarmante es que cuando un atacante explota el servidor de servicio de modelos, puede acceder y modificar datos sensibles que circulan hacia adentro y hacia afuera del servidor TorchServe de destino, socavando la confianza y la credibilidad de la aplicación».*