Investigadores de la Universidad de Minnesota se disculparon con los mantenedores del Linux Kernel Project este sábado por incluir de forma intencional vulnerabilidades en el código del proyecto, lo que llevó a que se prohibiera a la escuela a contribuir al proyecto de código abierto en el futuro.

> *«Si bien nuestro objetivo era mejorar la seguridad de Linux, ahora entendemos que fue perjudicial para la comunidad convertirlo en un tema de nuestra investigación y desperdiciar su esfuerzo revisando estos parches sin su conocimiento o permiso»,* dijo el profesor asistente Kangjie Lu, y los estudiantes graduados Qiushi Wu y Aditya Pakki.
>
> *«Lo hicimos porque sabíamos que no podíamos pedir permiso a los responsables de Linux, o estarían al acecho de los parches hipócritas»,* agregaron.

La disculpa surge de un estudio sobre lo que se llama *«compromisos hipócritas»*, que se publicó a inicios de febrero. El proyecto tenía como objetivo agregar deliberadamente vulnerabilidades de uso libre al kernel de Linux en nombre de la investigación de seguridad, aparentemente en un intento de resaltar cómo el código potencialmente malicioso podría escabullirse más allá del proceso de aprobación y, como consecuencia, sugerir formas de mejorar la seguridad del proceso de parcheo.

Un documento de aclaración previamente compartido por los académicos el 15 de diciembre de 2020 declaró que la junta de ética in investigación de la universidad revisó el estudio y determinó que no se trataba de una investigación en humanos.

Aunque los investigadores afirmaron que *«no introdujimos ni pretendemos introducir ningún error o vulnerabilidad en el OSS»,* el hecho es que surgió evidencia de lo contrario, lo que implica que la investigación se llevó a cabo sin una supervisión adecuada, y puso en riesgo la seguridad del kernel, llevando a una prohibición unilateral de envíos de código de cualquier persona que utilice una dirección de correo electrónico «umn.edu», además de invalidar todo

el código anterior enviado por los investigadores de la universidad.

> *«Nuestra comunidad no aprecia que se experimente y que se 'pruebe' mediante el envío de parches conocidos que no hacen nada a propósito o introducen errores a propósito»,* dijo Greg Kroah-Hartman, mantenedor del kernel de Linux.

Después del incidente, el Departamento de Ciencias de la Computación e Ingeniería de la Universidad, dijo que estaba investigando el incidente y agregó que que investigó el *«método de investigación y el proceso por el cual se aprobó este método de investigación, determinar las medidas correctivas apropiadas y protegerse contra problemas futuros».*

> *«Esto es peor que simplemente experimentar, esto es como decir que eres un investigador de seguridad yendo a una tienda de comestibles y cortando las líneas de los frenos de todos los autos para ver cuántas personas chocan cuando se van. Muy poco ético»,* dijo Jered Floyd.

Mientras tanto, se espera que todos los parches enviados al código base por los investigadores y profesores de la universidad sean revertidos y revisados nuevamente para verificar si son correcciones válidas.