Se ha compartido en línea un código de prueba de concepto (PoC) que demuestra una vulnerabilidad de omisión de firma digital recientemente revelada en Java. La vulnerabilidad de alta gravedad, CVE-2022-21449 tiene una puntuación CVSS de 7.5 y afecta a las versiones que se enlistan a continuación de Java SE y Oracle GraalVM Enterprise Edition.

- Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18
- Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1, 22.0.0.2

El problema reside en la implementación de Java del algoritmo de firma digital de curva elíptica (ECDSA), un mecanismo criptográfico para firmar de forma digital mensajes y datos para verificar la autenticidad y la integridad de los contenidos.

En otras palabras, el error criptográfico, denominado como Psychic Signatures en Java, hace posible presentar una firma totalmente en blanco, que aún sería percibida como válida por la implementación vulnerable.

La explotación exitosa de la falla podría permitir a un atacante falsificar firmas y eludir las medidas de autenticación implementadas.

El PoC, que fue publicado por el investigador de seguridad Khaled Nassar, involucra a un cliente vulnerable y un servidor TLS malicioso, el primero de los cuales acepta una firma no válida del servidor, lo que permite que el protocolo de enlace TLS siga sin obstáculos.

«Es difícil exagerar la gravedad de este error», dijo el investigador de ForgeRock, Neil Madden, quien descubrió e informó sobre la vulnerabilidad el 11 de noviembre de 2021.

> *«Se está utilizando firmas ECDSA para cualquiera de estos mecanismos de seguridad, entonces un atacante puede pasarlos por alto de forma trivial y completa si su servidor ejecuta cualquier versión de Java 15, 16, 17 o 18».*

Desde entonces, Oracle ha abordado el problema como parte de su actualización de parche

crítico (CPU) trimestral de abril de 2022 lanzada en 19 de abril de 2022.

A la luz del lanzamiento de la PoC, se recomienda a las organizaciones que utilizan Java 15, Java 16, Java 17 o Java 18 en sus entornos, que prioricen los parches para mitigar la explotación activa.