Los expertos en ciberseguridad han descubierto una forma de eludir una vulnerabilidad recientemente solucionada y activamente explotada en algunas versiones de Ivanti Endpoint Manager Mobile (EPMM), lo que ha llevado a Ivanti a instar a los usuarios a actualizar a la versión más reciente del software.

Conocido como CVE-2023-35082 (puntuación CVSS: 10.0) y descubierto por Rapid7, el problema *«permite a atacantes no autenticados acceder a la API en versiones antiguas sin soporte de MobileIron Core (11.2 y anteriores)».*

> *«Si se aprovecha, esta vulnerabilidad permite a un actor no autorizado y remoto (accesible desde internet) acceder potencialmente a la información de identificación personal de los usuarios y realizar cambios limitados en el servidor»,* explicó Ivanti en un aviso publicado el 2 de agosto de 2023.

El proveedor de servicios de software también afirmó que esta deficiencia fue «resuelta incidentalmente» en MobileIron Core 11.3 como parte del trabajo en una corrección de errores del producto y que previamente no había sido identificada como una falla de seguridad.

El investigador de seguridad de Rapid7, Stephen Fewer, dijo: *«CVE-2023-35082 surge del mismo origen que CVE-2023-35078, específicamente debido a la naturaleza permisiva de ciertas entradas en la cadena de filtros de seguridad de la aplicación web mifs».*

Esto también significa que CVE-2023-35081 podría ser utilizado en conjunto con CVE-2023-35082 *«para permitir que un atacante escriba archivos de webshell maliciosos en el dispositivo, que luego podrían ser ejecutados por el atacante».*

Con esta última revelación, Ivanti ha solucionado un total de tres fallos de seguridad que afectan a su producto EPMM en rápida sucesión en un lapso de dos semanas.

También coincide con el hecho de que agencias de ciberseguridad de Noruega y Estados

Unidos han informado que CVE-2023-35078 y CVE-2023-35081 han sido explotados por grupos de naciones no identificados, al menos desde abril de 2023, con el propósito de implantar web shells y obtener acceso remoto persistente a sistemas comprometidos.

- CVE-2023-35078 (calificación CVSS: 10.0) – Se trata de una vulnerabilidad de elusión de autenticación en Ivanti EPMM que permite a usuarios no autorizados acceder a funcionalidades o recursos restringidos de la aplicación sin la debida autenticación.

- CVE-2023-35081 (calificación CVSS: 7.2) – Se ha descubierto una vulnerabilidad de travesía de directorios en Ivanti EPMM que posibilita que un atacante escriba archivos arbitrarios en el dispositivo.

Aunque no se ha encontrado evidencia de explotación activa de CVE-2023-35082 en la naturaleza, se recomienda a los usuarios actualizar a la última versión compatible para protegerse de posibles amenazas.

> *«Ivanti EPMM 11.2 ha estado fuera de soporte desde el 15 de marzo de 2022. Por lo tanto, Ivanti no lanzará un parche ni otras soluciones para abordar esta vulnerabilidad en las versiones 11.2 o anteriores»,* indicó Ivanti.