Se han informado de múltiples fallos de seguridad críticos en Ivanti Avalanche, una solución de gestión de dispositivos móviles empresariales que utilizan 30,000 organizaciones.

Las vulnerabilidades, agrupadas bajo el seguimiento colectivo CVE-2023-32560 (puntuación CVSS: 9.8), son desbordamientos de búfer basados en la pila en el archivo Ivanti Avalanche WLAvanacheServer.exe v6.4.0.0.

La empresa de ciberseguridad Tenable indicó que estas debilidades resultan de desbordamientos de búfer que ocurren como consecuencia del procesamiento de tipos de datos específicos.

Un atacante remoto no autenticado puede especificar una cadena hexadecimal larga o un elemento de tipo 9 largo para sobrepasar el búfer, señaló.

La explotación exitosa de ambas cuestiones podría ser utilizada por un adversario remoto para lograr la ejecución de código o un colapso del sistema.

Las vulnerabilidades de desbordamiento de búfer basadas en la pila se presentan cuando el búfer que se está sobrescribiendo se encuentra en la pila, lo que da lugar a una situación en la que la ejecución del programa puede ser modificada para ejecutar código arbitrario con privilegios elevados.

Ivanti ha lanzado la versión 6.4.1 de Avalanche para solucionar el problema después de que se hiciera público en abril de 2023.

La actualización también aborda otras seis debilidades (desde CVE-2023-32561 hasta CVE-2023-32566) que podrían abrir el camino para eludir la autenticación y lograr la ejecución remota de código.

Dado que se han estado explorando activamente debilidades de seguridad en el software de Ivanti en las últimas semanas, es fundamental que los usuarios actúen con rapidez para aplicar las correcciones y así reducir las posibles amenazas.