El proveedor de servicios de software Ivanti está emitiendo una advertencia acerca de una nueva vulnerabilidad crítica de día cero que afecta al Ivanti Sentry, antes conocido como MobileIron Sentry. Según informa, esta vulnerabilidad se encuentra siendo activamente explotada en entornos en la naturaleza, lo que representa un aumento significativo en los problemas de seguridad de la empresa.

Identificada bajo la designación CVE-2023-38035 (con una puntuación CVSS de 9.8), esta problemática se describe como un caso de evasión de autenticación que afecta a las versiones 9.18 y anteriores. Esto se debe a lo que han llamado una configuración del Apache HTTPD que no es lo suficientemente restrictiva.

> *«En caso de ser explotada, esta vulnerabilidad permite que un actor sin autenticar tenga acceso a ciertas API sensibles que se utilizan para configurar el Ivanti Sentry en el portal de administración (puerto 8443, que comúnmente se denomina MICS)»*, afirmó la compañía.

> *«Aunque esta vulnerabilidad tiene una alta puntuación CVSS, existe un bajo riesgo de explotación para los clientes que no exponen el puerto 8443 a Internet».*

Una explotación exitosa de este fallo podría permitir a un atacante modificar la configuración, ejecutar comandos del sistema o escribir archivos en el sistema. Se recomienda a los usuarios limitar el acceso a MICS únicamente a las redes internas de gestión.

Aunque en la actualidad no se conocen detalles precisos acerca de cómo se está llevando a cabo la explotación, la empresa ha afirmado que solo tiene conocimiento de que un número limitado de clientes se han visto afectados.

La compañía noruega de ciberseguridad mnemonic ha sido reconocida por descubrir y reportar esta vulnerabilidad.

> *«La explotación exitosa permite a un actor sin autenticar leer y escribir archivos en el servidor de Ivanti Sentry y ejecutar comandos del sistema como administrador del sistema (root) mediante el uso de 'super usuario' (sudo)»,* declararon.

Además, CVE-2023-38035 podría ser utilizado como arma después de aprovechar CVE-2023-35078 y CVE-2023-35081, otras dos vulnerabilidades recientemente divulgadas en el Ivanti Endpoint Manager Mobile (EPMM). Esto sería aplicable en situaciones en las que el puerto 8443 no esté públicamente accesible, ya que el portal de administración se utiliza para comunicarse con el servidor de Ivanti EPMM.

Este desarrollo se presenta una semana después de que Ivanti solucionara dos graves fallos de desbordamiento de búfer en su software Avalanche (CVE-2023-32560) que podrían llevar a bloqueos y a la ejecución de código arbitrario en instalaciones vulnerables.