Mitel ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en MiVoice MX-ONE que podría permitir a un atacante evadir los mecanismos de autenticación.

"Se ha detectado una falla de omisión de autenticación en el componente Provisioning Manager de Mitel MiVoice MX-ONE que, si es aprovechada exitosamente, permitiría a un atacante sin credenciales evadir los controles de acceso debido a una gestión inadecuada de permisos," señaló la empresa en un aviso emitido el miércoles.

"Una explotación exitosa de esta debilidad podría otorgar al atacante acceso no autorizado a cuentas de usuario o administrador dentro del sistema."

Esta vulnerabilidad, que aún no cuenta con un identificador CVE asignado, posee una puntuación CVSS de 9.4 sobre un máximo de 10. Afecta a las versiones de MiVoice MX-ONE desde la 7.3 (7.3.0.0.50) hasta la 7.8 SP1 (7.8.1.0.14).

Los parches correspondientes han sido distribuidos bajo los identificadores MXO-15711_78SP0 y MXO-15711_78SP1 para las versiones 7.8 y 7.8 SP1, respectivamente. Se recomienda a los clientes que utilicen MiVoice MX-ONE desde la versión 7.3 en adelante que soliciten el parche a su proveedor de servicios autorizado.

Como medidas de mitigación mientras se aplican las correcciones, se sugiere restringir la exposición directa de los servicios MX-ONE a internet y asegurarse de que operen dentro de una red de confianza.

Además de la falla de autenticación, Mitel también ha lanzado correcciones para una vulnerabilidad de alta gravedad en MiCollab (CVE-2025-52914, con una puntuación CVSS de 8.8) que podría permitir a un atacante autenticado ejecutar un ataque de inyección SQL.

"Una explotación exitosa de esta vulnerabilidad permitiría al atacante acceder a datos de aprovisionamiento de usuarios y ejecutar comandos SQL arbitrarios, lo cual comprometería la confidencialidad, integridad y disponibilidad del sistema," indicó Mitel.

La vulnerabilidad afecta a las versiones de MiCollab desde la 10.0 (10.0.0.26) hasta la 10.0 SP1 FP1 (10.0.1.101), así como a la 9.8 SP3 (9.8.3.1) y versiones anteriores. El problema ha sido resuelto en las versiones 10.1 (10.1.0.10), 9.8 SP3 FP1 (9.8.3.103) y posteriores.

Dado el historial de ataques dirigidos a dispositivos Mitel, es crucial que los usuarios actualicen sus sistemas lo antes posible para reducir los riesgos de seguridad.