Investigadores en ciberseguridad han desarrollado un exploit de prueba de concepto (PoC) que combina una vulnerabilidad crítica previamente corregida en Mitel MiCollab con un día cero de lectura arbitraria de archivos. Esto podría permitir a un atacante acceder a archivos de instancias vulnerables.

La vulnerabilidad crítica, identificada como CVE-2024-41713 (puntuación CVSS: 9.8), se debe a una validación inadecuada de entradas en el componente NuPoint Unified Messaging (NPM) de Mitel MiCollab, lo que facilita un ataque de travesía de directorios.

MiCollab es una solución integrada de hardware y software que une funcionalidades de chat, voz, video y mensajería SMS, conectándose con Microsoft Teams y otras aplicaciones. El componente NPM es un sistema de correo de voz basado en servidor que permite acceder a los mensajes de voz de diversas formas, ya sea remotamente o a través de Microsoft Outlook.

De acuerdo con WatchTowr Labs, que compartió su análisis, CVE-2024-41713 fue descubierta mientras investigaban CVE-2024-35286 (también con puntuación CVSS: 9.8), otra vulnerabilidad crítica en el componente NPM que podría permitir a los atacantes extraer información confidencial y ejecutar operaciones arbitrarias sobre bases de datos y sistemas de administración.

Mitel corrigió esta falla de inyección SQL a finales de mayo de 2024 al lanzar la versión 9.8 SP1 (9.8.1.5) de MiCollab.

Detalles técnicos

Esta nueva vulnerabilidad destaca porque permite enviar el patrón `"..;/"` en solicitudes HTTP dirigidas al componente ReconcileWizard, logrando que los atacantes accedan al directorio raíz del servidor de aplicaciones y a datos confidenciales (como `/etc/passwd`) sin autenticación.

WatchTowr Labs también identificó que este bypass de autenticación puede combinarse con

una vulnerabilidad no corregida de lectura arbitraria de archivos posterior a la autenticación, permitiendo extraer información sensible.

Según Mitel, un ataque exitoso podría dar acceso no autorizado, comprometiendo la confidencialidad, integridad y disponibilidad del sistema. Además, un atacante podría acceder a información de configuración no sensible, realizar acciones administrativas no autorizadas y potencialmente afectar gravemente al servidor MiCollab.

La vulnerabilidad CVE-2024-41713 fue corregida en la versión 9.8 SP2 (9.8.2.12) o superior, publicada el 9 de octubre de 2024.

Reflexiones de los expertos

> El investigador Sonny Macdonald señaló:
> *«Este caso ha demostrado lo importante que es investigar vulnerabilidades incluso sin acceso al código fuente completo. Con una descripción detallada del CVE y habilidades avanzadas de búsqueda en línea, es posible identificar fallos de seguridad en soluciones comerciales de software».*

La versión 9.8 SP2 (9.8.2.12) también corrigió una vulnerabilidad de inyección SQL en el componente de conferencias de audio, web y video (AWV, CVE-2024-47223, puntuación CVSS: 9.4), que podría exponer información sensible o permitir consultas arbitrarias en bases de datos, comprometiendo la funcionalidad del sistema.

Casos relacionados

En un caso aparte, Rapid7 documentó varias vulnerabilidades en la cámara de seguridad Lorex 2K Indoor Wi-Fi, registradas como CVE-2024-52544 a CVE-2024-52548, que podrían usarse en conjunto para ejecutar código de forma remota (RCE).

En un escenario de ataque, las primeras tres fallas podrían emplearse para restablecer la

contraseña de administrador del dispositivo, mientras que las dos restantes permitirían ejecutar comandos en el sistema operativo con privilegios elevados.

> El investigador Stephen Fewer explicó:
> *«La cadena de explotación incluye cinco fallos distintos, que trabajan juntos en dos fases. La primera omite la autenticación, permitiendo a un atacante remoto restablecer la contraseña de administrador. La segunda aprovecha esta brecha para desbordar un búfer en la pila y ejecutar comandos con privilegios de root».*