Cisco ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica que afecta a su plataforma Identity Services Engine (ISE). Esta falla, si es aprovechada con éxito, podría permitir que actores no autenticados realicen acciones maliciosas en sistemas vulnerables.

El fallo de seguridad, identificado como CVE-2025-20286, tiene una puntuación CVSS de 9.9 sobre 10, y se clasifica como una vulnerabilidad por credenciales estáticas.

> "Una vulnerabilidad en las implementaciones en la nube de Cisco Identity Services Engine (ISE) en Amazon Web Services (AWS), Microsoft Azure y Oracle Cloud Infrastructure (OCI) podría permitir a un atacante remoto y no autenticado acceder a datos sensibles, ejecutar operaciones administrativas limitadas, modificar configuraciones del sistema o interrumpir servicios dentro de los sistemas afectados", indicó la empresa en un comunicado oficial.

Cisco, que atribuye el descubrimiento del fallo a Kentaro Kawane de GMO Cybersecurity, ha confirmado la existencia de un exploit de tipo prueba de concepto (PoC). No obstante, no hay indicios de que haya sido utilizado de forma maliciosa en entornos reales.

La raíz del problema reside en que, durante la instalación de Cisco ISE en entornos en la nube, las credenciales se generan incorrectamente. Como resultado, múltiples despliegues comparten las mismas credenciales siempre que la versión del software y la plataforma en la nube coincidan.

En otras palabras, las credenciales estáticas están vinculadas a cada combinación específica de versión y plataforma, pero no son intercambiables entre diferentes versiones o plataformas. Por ejemplo, según Cisco, todas las instancias de Cisco ISE versión 3.1 en AWS compartirán las mismas credenciales.

Sin embargo, esas mismas credenciales no serán válidas para acceder a una instancia con la versión 3.2, incluso si se encuentra en la misma plataforma. Además, la versión 3.2 en AWS

no tendrá las mismas credenciales que la misma versión en Azure.

El aprovechamiento exitoso de esta debilidad podría permitir a un atacante obtener credenciales de usuario de una instancia de ISE en la nube y usarlas para acceder a otros entornos de ISE en la nube mediante puertos no asegurados.

Esto podría dar lugar a accesos no autorizados a datos confidenciales, cambios en la configuración del sistema, interrupciones del servicio o la ejecución de tareas administrativas con privilegios limitados. Cabe destacar que la vulnerabilidad solo afecta a entornos donde el nodo principal de administración (Primary Administration Node) se ejecuta en la nube. Los despliegues en local (on-premises) no están comprometidos.

Las versiones afectadas son:

- AWS: Cisco ISE 3.1, 3.2, 3.3 y 3.4
- Azure: Cisco ISE 3.2, 3.3 y 3.4
- OCI: Cisco ISE 3.2, 3.3 y 3.4

No existe una solución temporal para CVE-2025-20286, pero Cisco sugiere limitar el tráfico a administradores autorizados o ejecutar el comando "`application reset-config ise`" para restablecer las contraseñas de usuario. No obstante, es importante advertir que este comando restablecerá Cisco ISE a su configuración de fábrica.