Ivanti ha alertado sobre tres nuevas vulnerabilidades de seguridad que afectan su Cloud Service Appliance (CSA), las cuales están siendo explotadas activamente.

Estas vulnerabilidades de día cero están siendo aprovechadas en combinación con otra falla en el CSA que la compañía corrigió el mes pasado, según informó el proveedor de servicios de software con sede en Utah.

Si se explotan con éxito, estas vulnerabilidades podrían permitir a un atacante autenticado con privilegios de administrador eludir restricciones, ejecutar comandos SQL arbitrarios o lograr la ejecución remota de código.

> *«Tenemos conocimiento de un número limitado de clientes que ejecutan CSA versión 4.6 con parche 518 y anteriores que han sido atacados cuando las vulnerabilidades CVE-2024-9379, CVE-2024-9380 o CVE-2024-9381 se combinan con CVE-2024-8963«,* mencionó la empresa.

No se ha encontrado evidencia de explotación en entornos que utilizan CSA versión 5.0. A continuación, se ofrece una descripción breve de las tres vulnerabilidades:

- CVE-2024-9379 (puntuación CVSS: 6.5): Inyección SQL en la consola web de administración de Ivanti CSA anterior a la versión 5.0.2, que permite a un atacante remoto autenticado con privilegios de administrador ejecutar comandos SQL arbitrarios.
- CVE-2024-9380 (puntuación CVSS: 7.2): Vulnerabilidad de inyección de comandos en el sistema operativo desde la consola web de administración de Ivanti CSA anterior a la versión 5.0.2, que permite a un atacante remoto autenticado con privilegios de administrador ejecutar código remotamente.
- CVE-2024-9381 (puntuación CVSS: 7.2): Vulnerabilidad de recorrido de directorios (path traversal) en Ivanti CSA anterior a la versión 5.0.2, que permite a un atacante remoto autenticado con privilegios de administrador eludir las restricciones de acceso.

Los ataques detectados por Ivanti combinan estas vulnerabilidades con CVE-2024-8963 (puntuación CVSS: 9.4), una vulnerabilidad crítica de recorrido de directorios que permite a un atacante remoto sin autenticación acceder a funcionalidades restringidas.

Ivanti descubrió estas tres vulnerabilidades como parte de su investigación sobre la explotación de CVE-2024-8963 y CVE-2024-8190 (puntuación CVSS: 7.2), otra vulnerabilidad de inyección de comandos en el sistema operativo que también ha sido explotada y ya ha sido parcheada.

Además de actualizar a la versión más reciente (5.0.2), Ivanti recomienda a los usuarios revisar los dispositivos en busca de cuentas administrativas modificadas o agregadas recientemente para detectar signos de intrusión, o verificar alertas de herramientas de detección y respuesta en los endpoints (EDR) instaladas en el dispositivo.

Este anuncio llega menos de una semana después de que la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) agregara una vulnerabilidad que afecta a Ivanti Endpoint Manager (EPM) y que fue corregida en mayo (CVE-2024-29824, puntuación CVSS: 9.6) al catálogo de Vulnerabilidades Conocidas Explotadas (KEV).