Fortinet ha publicado correcciones para una vulnerabilidad crítica que afecta a FortiWeb, la cual podría permitir que un atacante no autenticado ejecute comandos arbitrarios en la base de datos en instancias vulnerables.

Identificada como CVE-2025-25257, esta falla cuenta con una puntuación CVSS de 9.6 sobre un máximo de 10.0.

"Una neutralización inadecuada de elementos especiales utilizados en una instrucción SQL ('Inyección SQL') [CWE-89] en FortiWeb podría permitir que un atacante no autenticado ejecute código SQL no autorizado a través de solicitudes HTTP o HTTPS manipuladas," señaló Fortinet en un aviso emitido esta semana.

La vulnerabilidad afecta a las siguientes versiones:

- FortiWeb de la 7.6.0 a la 7.6.3 (Actualizar a la 7.6.4 o superior)
- FortiWeb de la 7.4.0 a la 7.4.7 (Actualizar a la 7.4.8 o superior)
- FortiWeb de la 7.2.0 a la 7.2.10 (Actualizar a la 7.2.11 o superior)
- FortiWeb de la 7.0.0 a la 7.0.10 (Actualizar a la 7.0.11 o superior)

Kentaro Kawane, de GMO Cybersecurity, quien recientemente fue reconocido por reportar una serie de fallos críticos en Cisco Identity Services e ISE Passive Identity Connector (CVE-2025-20286, CVE-2025-20281 y CVE-2025-20282), ha sido acreditado como el descubridor de esta vulnerabilidad.

Según un análisis publicado hoy por watchTowr Labs, el problema radica en una función llamada *"get_fabric_user_by_token"*, vinculada al componente Fabric Connector, el cual sirve como puente entre FortiWeb y otros productos de Fortinet.

Esta función es invocada por otra función denominada *"fabric_access_check"*, la cual es llamada desde tres diferentes puntos de acceso API: */api/fabric/device/status*, */api/v[0-9]/fabric/widget/[a-z]+* y */api/v[0-9]/fabric/widget*.

El problema ocurre porque los datos controlados por el atacante —enviados mediante un encabezado de autorización Bearer token dentro de una solicitud HTTP especialmente diseñada— se transfieren directamente a una consulta SQL sin una sanitización adecuada que garantice que no contengan código malicioso.

El ataque podría escalar a ejecución remota de código si se incorpora una instrucción *SELECT … INTO OUTFILE* para escribir una carga maliciosa en un archivo del sistema operativo subyacente, aprovechando el hecho de que la consulta se ejecuta con privilegios del usuario "mysql", pudiendo activarse posteriormente con Python.

"La nueva versión de la función sustituye la antigua consulta con formato de cadena por sentencias preparadas – un intento razonable para evitar inyecciones SQL directas," afirmó el investigador de seguridad Sina Kheirkhah.

Como medida temporal hasta que se apliquen los parches correspondientes, se recomienda a los usuarios desactivar la interfaz administrativa HTTP/HTTPS.

Dado que en ocasiones anteriores actores maliciosos han explotado vulnerabilidades en dispositivos Fortinet, es crucial que los usuarios actualicen a la versión más reciente lo antes posible para reducir riesgos potenciales.