Se revelaron múltiples vulnerabilidades de alta gravedad en la solución de administración de contraseñas PasswordState, que podría ser explotada por un atacante remoto no autenticado para obtener las contraseñas de texto sin formato de un usuario.

> *«La explotación exitosa permite que un atacante no autenticado extraiga contraseñas de una instancia, sobrescriba todas las contraseñas almacenadas dentro de la base de datos o eleve sus privilegios dentro de la aplicación»*, dijo la compañía suiza de seguridad cibernética Modzero AG.

> *«Algunas de las vulnerabilidades individuales se pueden encadenar para obtener un shell en el sistema host de Passwordstate y volcar todas las contraseñas almacenadas en texto claro, comenzando con nada más que un nombre de usuario válido».*

Passwordstate, desarrollado por una empresa australiana llamada Click Studios, tiene más de 29,000 clientes y lo utilizan más de 370,000 profesionales de TI.

Una de las vulnerabilidades también afecta a la versión 9.5.8.4 de Passwordstate para el navegador web Chrome. La última versión del complemento del navegador es 9.6.1.2, que se lanzó el 7 de septiembre de 2022.

La lista de vulnerabilidades identificadas por modzero AG es la siguiente:

- CVE-2022-3875 (puntaje CVSS: 9.1): Omisión de autenticación para la API de Passwordstate
- CVE-2022-3876 (puntaje CVSS: 6.5): Omisión de los controles de acceso a través de claves controladas por el usuario
- CVE-2022-3877 (puntaje CVSS: 5.7): Una vulnerabilidad de secuencias de comandos entre sitios almacenada en el campo URL de cada entrada de contraseña

- Sin CVE (Puntaje CVSS: 6.0): Un mecanismo insuficiente para proteger las contraseñas mediante el uso de cifrado simétrico del lado del servidor
- Sin CVE (puntaje CVSS: 5.3): Uso de credenciales codificadas para enumerar eventos auditados, como solicitudes de contraseña y cambios de cuenta de usuario por medio de la API
- Sin CVE (puntaje CVSS: 4.3): Uso de credenciales insuficientemente protegidas para listas de contraseñas

Explotar las vulnerabilidades podría permitir que un atacante con conocimiento de un nombre de usuario válido extraiga contraseñas guardadas en texto no cifrado, sobrescriba las contraseñas en la base de datos e incluso eleve los privilegios para lograr la ejecución remota de código.

Además, un flujo de autorización inadecuado (puntuación CVSS: 3.7) identificado en la extensión del navegador Chrome podría convertirse en un arma para enviar todas las contraseñas a un dominio controlado por el hacker.

En una cadena de ataque demostrada por modzero AG, un actor de amenazas podría falsificar un token API para una cuenta de administrador y explotar la falla XSS para agregar una entrada de contraseña maliciosa para obtener un shell inverso y obtener las contraseñas alojadas en la instancia.

Se recomienda a los usuarios de Passwordstate actualizar a la versión 9.6 Build 9563 lanzada el 7 de noviembre de 2022 o versiones posteriores para mitigar las amenazas potenciales.

Passwordstate fue víctima de un ataque a la cadena de suministro en abril de 2021, dicho ataque cibernético permitió a los hackers aprovechar el mecanismo de actualización del servicio para colocar una puerta trasera en las máquinas de los clientes.