La compañía de alojamiento web GoDaddy, reveló el lunes pasado una violación de datos que resultó en el acceso no autorizado a datos personales de 1.2 millones de clientes activos e inactivos, lo que lo convierte en el tercer incidente de seguridad que sale a la luz desde 2018.

En una presentación ante la Comisión de Bolsa y Valores de Estados Unidos (SEC), el registrador de dominios más grande del mundo dijo que un tercero malicioso logró obtener acceso a su entorno de alojamiento de WordPress administrado el pasado 6 de septiembre, con la ayuda de una contraseña comprometida, usándola para obtener información sensible de sus clientes. No se sabe si la contraseña comprometida se protegió con autenticación de dos factores.

GoDaddy cuenta con más de 20 millones de clientes, con más de 82 millones de nombres de dominio registrados usando sus servicios.

La compañía dijo que descubrió el problema el 17 de noviembre. Se está llevando a cabo una investigación sobre el incidente y la compañía dijo que está *«contactando a todos los clientes afectados directamente con detalles específicos».* Se cree que el intruso accedió a la siguiente información:

- Direcciones de correo electrónico y números de clientes de hasta 1.2 millones de clientes de WordPress administrados activos e inactivos.
- Se expuso la contraseña de administrador de WordPress original que se estableció en el momento del aprovisionamiento.
- sFTP y nombres de usuario y contraseñas de bases de datos asociados con sus clientes activos e inactivos.
- Claves privadas SSL para un subconjunto de clientes activos.

GoDaddy dijo que está en proceso de emisión e instalación de nuevos certificados para los clientes afectados. Como medida de precaución, la compañía también declaró que restableció las contraseñas afectadas y está reforzando su sistema de aprovisionamiento con protecciones de seguridad adicionales.

Según el director ejecutivo de Wordfence, Mark Maunder, *«GoDaddy almacenaba las contraseñas sFTP de tal forma que se podían recuperar las versiones de texto sin formato de las contraseñas, en lugar de almacenar salt hashes de estas contraseñas o proporcionar autenticación de clave pública, que son las mejores prácticas de la industria».*

Aunque las violaciones de datos ya no son una ocurrencia esporádica, la exposición de direcciones de correo electrónico y contraseñas presenta un riesgo de ataques de phishing, sin mencionar que permite a los atacantes violar los sitios vulnerables de WordPress para cargar malware y acceder a otra información de identificación personal almacenada en ellos.

> *«En los sitios donde se expuso la clave privada SSL, un atacante podría descifrar el tráfico utilizando la clave privada SSL robada, siempre que pudiera realizar con éxito un ataque man-in-the-middel (MiTM) que intercepte el tráfico cifrado entre un visitante del sitio y un sitio afectado»,* dijo Maunder.

Actualización

La violación de datos de GoDaddy puede ser más profunda de lo que la compañía ha estado dispuesta a admitir, como lo han hecho varias subsidiarias de los servicios administrados de WordPress de la empresa, como 123Reg, Domain Factory, Heart Internet, Host Europe, Media Temple y tsoHost, que se han encontrado afectados.

GoDaddy dijo a Wordfence que *«una pequeña cantidad de usuarios de WordPress administrados activos e inactivos en esas marcas se vieron afectados»,* aunque no está claro de forma exacta cuántos usuarios adicionales pudieron haber expuesto sus detalles confidenciales a raíz del incidente de seguridad.