Vulnerabilidad De GoDaddy Permitía El Secuestro De Dominios

GoDaddy, la **empresa de registro de dominios** y de alojamiento web ha solucionado un fallo de Cross-Site Request Forgery (CSRF or XSRF), el cual permitía a los atacantes informáticos secuestrar sitios web registrados con esta **empresa de registro de dominios**.

La vulnerabilidad fue reportada a GoDaddy el sábado por Dylan Saccomanni, un consultor de seguridad y penetración de aplicaciones web en Nueva York. Sin ningún tipo de retraso de tiempo, la compañía ha solucionado el fallo en menos de 24 horas después de la publicación del blog. Si bien la gestión de un viejo **dominio registrado en GoDaddy**, Saccomanni tropezó con el error y se dio cuenta que no había absolutamente ninguna protección contra la vulnerabilidad usando CSRF, en diferentes acciones de **gestión de DNS enGoDaddy**.

CSRF es un método para atacar un sitio web en el que un atacante necesita convencer a la víctima a hacer clic en un HTML especialmente diseñado, el cual hará una petición a la página web vulnerable para extraer la información necesaria. Este **grave fallo en GoDaddy** podría haber sido utilizado por los atacantes para **manipular la configuración de dominio** en cualquier sitio o incluso secuestrar todo el dominio sin ningún conocimiento de la víctima (el dueño de dominio).

> *«Un atacante puede aprovechar una vulnerabilidad CSRF para hacerse cargo de dominios registrados con GoDaddy,» Saccomanni escribió en su blog.*

Según el investigador, no había **token CSRF** presente en la solicitud o las cabeceras, y sin la aplicación de Referido,

los atacantes aprovecharon para publicar códigos necesarios para **editar servidores de nombres**, desactivar la auto-renovación y editar el archivo de zona.

Todos los atacantes tienen que hacer es aprovechar algún tipo de táctica de ingeniería social, a fin de aprovechar la vulnerabilidad CSRF.

> *«Ellos no necesitan información sensible acerca de la cuenta de la víctima, ya sea para auto renovarse y modificar los servidores de nombres», dijo Saccomanni. «Para la gestión de registro de DNS, todo lo que necesitas saber es el nombre de dominio de los registros DNS.»*

GoDaddy no dio inmediatamente respuesta sobre el tema, y mucho menos aclaro si las cuentas de usuarios habían sido comprometidas.

Saccomanni dijo que intentó **comunicarse con GoDaddy** usando muchas direcciones de correo electrónico diferentes relacionados con la seguridad y la ingeniería, así como la atención al cliente con el fin de informar de la falla. Después de recibir como respuesta, que no habría «ninguna línea de tiempo» para un parche, el día de ayer se dio cuenta de que se había solucionado este fallo en el **servicio de GoDaddy**.