ENPM686-0201

Samridha Murali

01/31/2022

Current Event 1

GoDaddy is one of the world's largest domain registrar and web hosting companies that provides services to more than 20 million customers worldwide. GoDaddy's managed wordpress hosting service got breached and personal data of more than 1.2 million users got exposed. This is the fourth time GoDaddy has faced a data breach in the last few years. Security team discovered the incident after spotting an altered SSH file in GoDaddy's hosting environment and suspicious activity on a subset of GoDaddy's server on November 17 2022, but the initial intrusion dates more than two month back. With a compromised password, an unauthorized third party accessed the provisioning system in their legacy code base.

Upto 1.2 million active and inactive customer's email addresses were exposed. WordPress Admin password was exposed. Active Users's FTP and database usernames and passwords were exposed. For some active customers, SSL private keys were exposed. Leaked credentials can be used to construct convincing phishing attacks which can lead to more dangerous consequences.

To avoid such breach,mulifactor authentication can be used. Even better, some secure authentication apps can be used. Importantly passwords should be kept as secure as possible. Round the clock intrusion detection and response activity could reduce the time gap between intrusion and detection of intrusion.