UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00229

GODADDY BREACH AFFECTS CUSTOMERS & RESELLERS

DATE ISSUED: 1st December 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Cyber incidents have plagued the high profile domain registrar GoDaddy who have reported their 5th breach since 2018 that occurred on 6th September affecting 1.2 million of its customers and down the supply chain after an attacker stole email addresses, SSH keys and database logins.

BREAKDOWN

The attacker who breached the giant and remained undetected for nearly two months in the Managed WordPress hosting environment kicking off an investigation involving forensic teams and law enforcement officials. The unauthorised third-party used a compromised password to gain access to the legacy code base for the system and were able to make off with emails, customer numbers, sFTO and database credential sets, and SSL private keys for a selection of currently active customers. With an on-going investigation still underway, few details as to the exact number of effected customers have been released. Speculation among researchers suggests that the attacker could use the private keys and certificates to hijack domains and cause reputational damage with impersonation sites and carry out further breaches down the supply chain. Various subsidiaries that resell GoDaddy Managed WordPress have also been affected: 123Red, Domain Factory, Heart Internet, Host Europe, Media Temple and tsoHost.

REMEDIATION STEPS

- Implement Multi-factor Authentication (MFA) wherever possible.
- Implement good key and password management practices. Incorporate cryptographic agility capapbility to enable quick rollover of certifications and keys.
- Grant access to users using the least-privilege and least access principles to lessen compromise.
- Reset any passwords believed to be compromised.
- Check certificates are updated and change passwords for sFTP access to new and unique passphrases.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/godaddys-latest-breach-customers/176530/
https://threatpost.com/godaddy-breach-widens-reseller-subsidiaries/176575/