Epic CA Fails

Prepare Now For The Inevitable

Over the past decade, we’ve seen a broad spectrum of Certificate Authority (CA) errors.

**Feb 2016**
Symantec: technology malfunction
Systems incorrectly parse email addresses, leaving them open to abuse

**July 2016**
Comodo: technology malfunction
Dangling markup injection issues, arbitrary wildcard certificates

**Mar 2018**
Trustico: business partner compromise
Reseller triggers immediate revocation by emailing 23,000 private keys

**Aug 2016**
WoSign: abuse of trust
CA is caught issuing certificates to non-domain owners

**Oct 2016**
GoDaddy: technology malfunction
Faulty upgrade allows certain servers to bypass the authentication process

**Sept 2017**
PROCERT: inadequate controls
CA is responsible for numerous issues centering around the misissuing of SSL certificates

**Jan 2017**
CrossCert: business partner compromise
Partner overrides Symantec compliance flags to bypass domain validations (Symantec intermediate)

**Mar 2011**
CertStar: business partner compromise
Comodo reseller bypasses security mechanism to misissue Mozilla.com certificate

**Dec 2008**
StartCom: hacker compromise
Breach causes CA to temporarily suspend certificate issuance

**Aug 2011**
DigiNota: hacker compromise
Hacked systems issue hundreds of fraudulent certificates

**Sept 2011**
GlobalSign: hacker compromise
CA voluntarily suspends operations while investigating breach

**Dec 2013**
ANSSI: business partner compromise
Subordinate CA misissues intermediate certificate, later abused by user

**July 2014**
CNNIC: abuse of trust
Unconstrained intermediate certificate is used for network interception

What's the potential impact of a CA error or compromise?

Certificate Authorities Aren't Perfect

What can you do about it?

Prepare now for the inevitable. Learn more about how Venafi can help you proactively manage all CAs and all keys and certificates.

Visit venafi.com