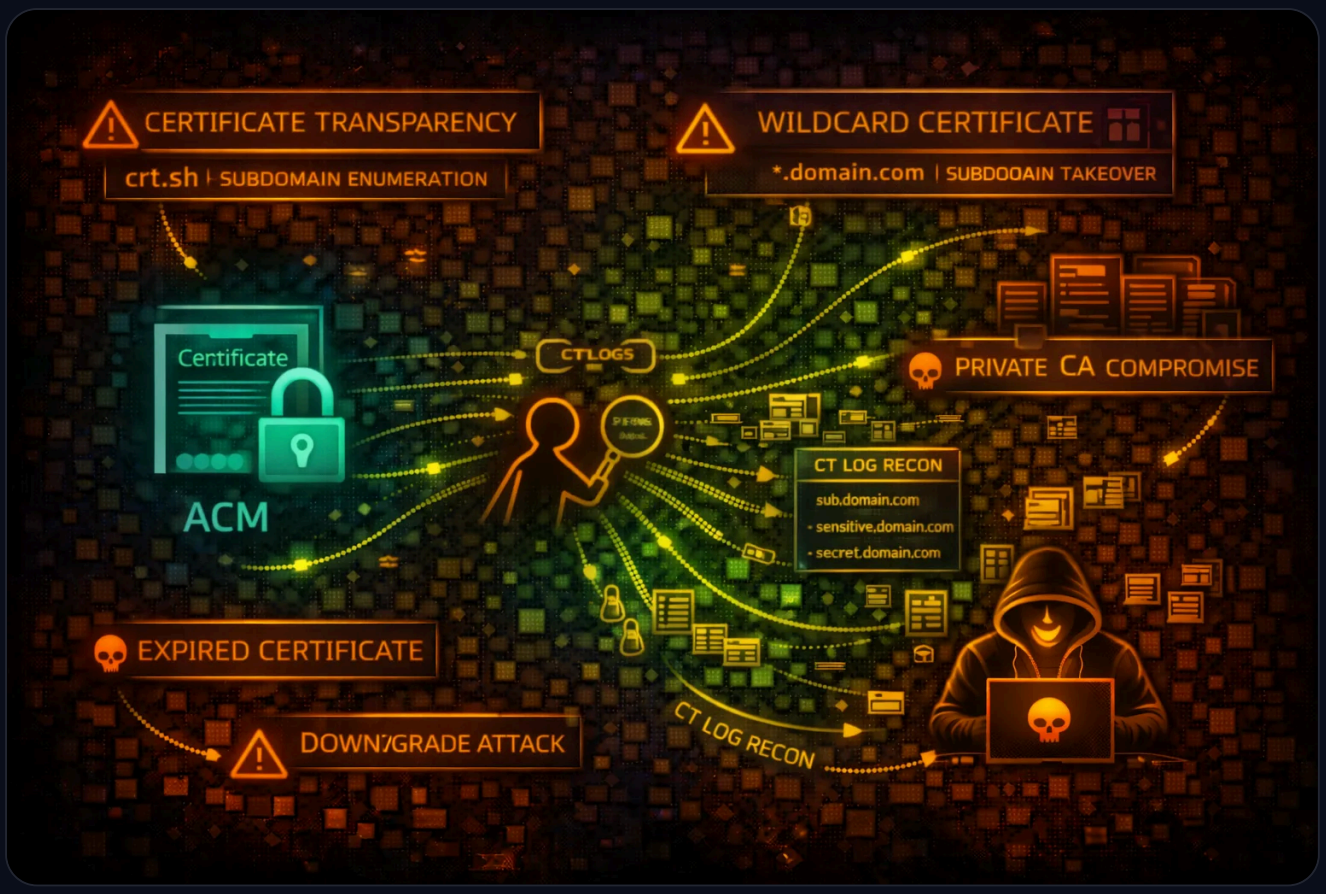

AWS ACM Security

CERTIFICATES

AWS Certificate Manager (ACM) handles provisioning, managing, and deploying SSL/TLS certificates. Certificates secure connections for ALB, CloudFront, API Gateway, and other AWS services.

MEDIUM	5+	TLS	FREE
Risk Level	Attack Vectors	Protocol	Public Certs

Service Overview

Public Certificates

Free SSL/TLS certificates for public-facing resources. Automatically renewed. Requires domain validation via DNS or email. Can only be used with integrated AWS services.

Integrations: ALB, NLB, CloudFront, API Gateway, Elastic Beanstalk, CloudFormation

Private Certificates

Private CA for internal resources. Requires AWS Private CA (additional cost). Private key can be exported for use outside AWS. Supports custom validity periods.

Use cases: Internal services, IoT devices, on-premises resources, containers, EC2 instances

Security Risk Assessment

5.5

Risk Score

ACM itself has limited direct attack surface, but certificate enumeration reveals infrastructure, and mismanaged private CAs can enable MITM attacks. Expired certificates cause service outages.

⚔️ Attack Vectors

Reconnaissance

- Certificate enumeration reveals domain inventory
- CT logs expose all issued certificates publicly
- SubjectAlternativeNames leak internal hostnames
- Wildcard certs reveal domain scope
- Certificate expiry dates for timing attacks

Exploitation

- Private CA compromise for MITM
- Stolen private keys enable impersonation
- DNS/email validation hijacking
- Certificate pinning bypass
- Exploiting expired certificate errors

⚠️ Misconfigurations

Certificate Issues

- Using self-signed certs in production
- Overly broad wildcard certificates
- Expired certificates causing outages
- Missing certificate renewal automation
- Weak cipher suites on services using cert

Private CA Issues

- Private CA key stored insecurely
- Overly permissive certificate issuance
- No certificate revocation checking
- Missing audit logging for CA operations
- Private keys exported without encryption

🔍 Enumeration

List All Certificates

```
aws acm list-certificates --region us-east-1
```

Describe Certificate Details

```
aws acm describe-certificate --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/xxx
```

List Tags for Certificate

```
aws acm list-tags-for-certificate --certificate-arn arn:aws:acm:...:certificate/xxx
```

List Private CAs

```
aws acm-pca list-certificate-authorities
```

Get CA Certificate

```
aws acm-pca get-certificate-authority-certificate --certificate-authority-arn arn:aws:acm-pca:...
```

🔎 CT Log Reconnaissance

Certificate Transparency

- All public ACM certs logged to CT
- Historical certificate data available
- Subdomain enumeration via crt.sh
- Internal hostnames in SAN fields exposed
- Staging/dev environment discovery

Query crt.sh for Domain

```
curl -s "https://crt.sh/?q=%.example.com&output=json" | jq -r '.[].name_value' | sort -u
```

OSINT Tip: CT logs are a goldmine for subdomain enumeration. Use crt.sh, censys.io, or certspotter to discover all issued certificates.

Private CA Attacks

CA Compromise Scenarios

- Issue rogue certificates for any domain
- Create backdoor certificates for MITM
- Sign malicious code with CA cert
- Disable certificate revocation
- Modify CA certificate templates

Post-Compromise Actions

- MITM internal service traffic
- Impersonate internal services
- Sign malware as trusted software
- Persist via long-lived certificates
- Access encrypted data streams

Detection

CloudTrail Events

- RequestCertificate - new cert request
- DeleteCertificate - cert deletion
- ExportCertificate - private key export
- IssueCertificate - private CA issuance
- RevokeCertificate - cert revocation
- CreateCertificateAuthority - new private CA

Monitoring

- Certificate expiration alerts
- Unusual certificate issuance patterns
- Private key export events
- CA configuration changes
- Failed validation attempts

💻 Exploitation Commands

Get All Certificate ARNs

```
aws acm list-certificates --query 'CertificateSummaryList[*].CertificateAr
n' --output text
```

Get Certificate Domains

```
aws acm list-certificates --query 'CertificateSummaryList[*].[DomainName,Su
bjectAlternativeNameSummaries]' --output table
```

Find Expiring Certificates

```
aws acm list-certificates --certificate-statuses ISSUED --query 'Certificat
eSummaryList[?NotAfter<=\`2024-12-31\`]'
```

Export Private Cert (if allowed)

```
aws acm export-certificate \\
  --certificate-arn arn:aws:acm:...:certificate/xxx \\
  --passphrase $(echo -n 'password' | base64)
```

CT Log Query - crt.sh

```
curl -s "https://crt.sh/?q=%.target.com&output=json" | \\
  jq -r '.[].name_value' | sort -u
```

Get Resources Using Cert

```
aws acm describe-certificate \\
  --certificate-arn arn:aws:acm:...:certificate/xxx \\
  --query 'Certificate.InUseBy'
```

📜 Policy Examples

✕ Overly Permissive ACM Access

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "acm:*",
    "Resource": "*"
  }]
}
```

Full ACM access allows certificate deletion, private key export, and private CA management

✓ Read-Only Certificate Access

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:ListTagsForCertificate"
    ],
    "Resource": "*"
  }]
}
```

Read-only access for monitoring and inventory purposes

✕ Dangerous Private CA Permissions

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm-pca:IssueCertificate",
      "acm-pca:GetCertificate"
    ],
    "Resource": "*"
  }]
}
```

Ability to issue certificates from any private CA enables MITM attacks

✓ Scoped Private CA Access

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["acm-pca:IssueCertificate"],
    "Resource": "arn:aws:acm-pca:*:*:certificate-authority/specific-ca
-id",
    "Condition": {
      "StringEquals": {
        "acm-pca:TemplateArn": "arn:aws:acm-pca:::template/EndEntityCe
rtificate/V1"
      }
    }
  }]
}
```

Restricted to specific CA and certificate template

Defense Recommendations

Monitor Certificate Expiration

Set up CloudWatch alarms for certificates expiring within 30 days.

```
aws cloudwatch put-metric-alarm \\
  --alarm-name CertExpiringSoon \\
  --metric-name DaysToExpiry \\
  --namespace AWS/CertificateManager \\
  --threshold 30 --comparison-operator LessThanThreshold
```

Restrict Export Permissions

Prevent private key export by denying acm:ExportCertificate action.

```
{
  "Effect": "Deny",
  "Action": "acm:ExportCertificate",
  "Resource": "*"
}
```

Use Separate Certs per Environment

Don't use the same wildcard certificate across prod/staging/dev.

Enable CloudTrail Logging

Log all ACM and ACM-PCA API calls for audit trail.

```
aws cloudtrail put-event-selectors \\
  --trail-name main-trail \\
  --event-selectors '[{"DataResources":[{"Type":"AWS::ACM::Certifi
cate"}]}]'
```

Secure Private CA

Use HSM-backed keys and restrict IssueCertificate permissions to specific templates.

Automate Certificate Renewal

Use DNS validation with Route 53 for automatic renewal without manual intervention.

```
aws acm request-certificate \\
  --domain-name example.com \\
  --validation-method DNS \\
  --domain-validation-options DomainName=example.com,ValidationDom
ain=example.com
```