**Kubernetes的TLS证书漏洞修复（DS）Kubeadm**

**1. 修改 Kubernetes API Server 的 TLS 配置**

Kubernetes API Server 的 TLS 配置可以通过修改 kube-apiserver 的启动参数来调整。

**步骤：**

1. 找到 kube-apiserver 的配置文件：

* 在 kubeadm 部署的集群中，kube-apiserver 的配置文件通常位于 /etc/kubernetes/manifests/kube-apiserver.yaml。

1. 编辑 kube-apiserver.yaml 文件：

|  |
| --- |
| Bash sudo vi /etc/kubernetes/manifests/kube-apiserver.yaml |

1. 在 spec.containers.command 部分添加或修改以下参数：

|  |
| --- |
| YAML - --tls-cipher-suites=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 - --tls-min-version=VersionTLS12 |

这些参数的作用：

* --tls-cipher-suites：指定安全的加密套件，禁用不安全的加密套件（如 3DES）。
* --tls-min-version：设置最低 TLS 版本为 TLS 1.2，禁用 TLS 1.0 和 TLS 1.1。

1. 保存并退出文件。
2. 重启 kube-apiserver：

* 由于 kube-apiserver 是以静态 Pod 方式运行的，修改配置文件后，Kubernetes 会自动重启该 Pod。
* 可以通过以下命令检查 kube-apiserver 的状态：

|  |
| --- |
| Bash kubectl get pods -n kube-system | grep apiserver |

**2. 验证 TLS 配置是否生效**

使用工具验证 Kubernetes API Server 的 TLS 配置是否已更新。

**使用 nmap 扫描：**

|  |
| --- |
| Bash nmap --script ssl-enum-ciphers -p 6443 <your-kubernetes-api-server-ip> |

检查输出，确保不再支持不安全的加密套件（如 3DES）。

**使用 openssl 测试：**

|  |
| --- |
| Bash openssl s\_client -connect <your-kubernetes-api-server-ip>:6443 -tls1\_2 |

检查输出，确认仅支持安全的加密套件。

**3. 更新 Ingress Controller 的 TLS 配置（如果适用）**

如果 Kubernetes 集群中使用了 Ingress Controller（如 Nginx Ingress 或 Traefik），也需要确保其 TLS 配置安全。

**以 Nginx Ingress 为例：**

1. 修改 Ingress Controller 的 ConfigMap：

|  |
| --- |
| YAML apiVersion: v1 kind: ConfigMap metadata:  name: nginx-configuration  namespace: ingress-nginx data:  ssl-ciphers: "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384"  ssl-protocols: "TLSv1.2 TLSv1.3" |

1. 重启 Ingress Controller 以应用更改。

**4. 更新其他组件的 TLS 配置**

确保 Kubernetes 集群中的其他组件（如 etcd、kubelet 等）也使用了安全的 TLS 配置。

**5. 定期更新 Kubernetes 版本**

Kubernetes 社区会定期修复安全漏洞，建议将集群升级到最新稳定版本，以获取最新的安全补丁。

**6. 使用安全扫描工具**

使用 Kubernetes 安全扫描工具（如 kube-bench 或 kube-hunter）检查集群的安全性，确保没有其他潜在漏洞。

通过以上步骤，可以有效修复 Kubernetes API Server 的 **SWEET32** 漏洞，并提升集群的整体安全性。