FM-KED-005 — SSL/TLS Certificate Expiration

Severity: S1 — Critical
Recovery Class: B — Standard Recovery
Covered by Monthly Support: Yes

Description

SSL/TLS certificates used by Finmars services expire, causing secure connections to fail and rendering applications inaccessible over HTTPS.

This issue is time-based and entirely recoverable through certificate renewal.

Typical Symptoms

- Browsers displaying certificate expiration warnings
- HTTPS connections rejected by clients or integrations
- API calls failing due to TLS handshake errors
- Monitoring alerts related to certificate validity

Diagnostic Checklist

Verify Certificate Expiration

```
openssl s_client -connect domain:443 -servername domain | openssl x509 -noout -dates
```

Identify Certificate Termination Point

- Nginx reverse proxy
- Kubernetes Ingress controller

Recovery Procedure

Follow the procedure relevant to the deployment model.

Option 1: Renew Certificate in Nginx Proxy

- Generate or obtain renewed certificate
- Replace certificate and private key in Nginx configuration
- Reload Nginx configuration

```
sudo nginx -t
sudo systemctl reload nginx
```

Option 2: Renew Certificate in Kubernetes Ingress

- Renew certificate via the configured certificate manager
- Update or recreate TLS secret used by the Ingress
- Verify Ingress reload and certificate propagation

Preventive Notes

- Track certificate expiration dates
- Use automated renewal where possible
- Monitor certificate validity proactively

Responsibility Boundary

Finmars SCSA provides best-effort renewal guidance and validation.
Certificate issuance authority availability and DNS control remain customer responsibilities.

Revision #1
Created 2026-01-07 14:33:15 UTC by Sergei Zhitenev
Updated 2026-01-07 14:34:38 UTC by Sergei Zhitenev