Security Advisory: Credential Rotation Required

Advisory ID: SA-2024-001 **Date:** June 15, 2024 **Severity:** Medium **Status:** Resolved **Author:** Security Team

---

Summary

On June 14, 2024, we identified that API credentials for a third-party logging service were inadvertently committed to a public repository. While we have no evidence of unauthorized access, we are requiring affected teams to rotate credentials as a precautionary measure.

What Happened

Timeline

Time (PT)	Event
Jun 14, 10:15	Automated secret scanning detected credentials in public repo
Jun 14, 10:18	Alert sent to Security team
Jun 14, 10:25	Repository made private
Jun 14, 10:30	Incident declared, investigation started
Jun 14, 11:00	Affected credentials identified
Jun 14, 11:30	Third-party vendor notified
Jun 14, 12:00	Credentials revoked at vendor
Jun 14, 14:00	New credentials issued
Jun 14, 16:00	All services updated
Jun 14, 17:00	Incident closed

Root Cause

A developer accidentally committed a configuration file containing API credentials to a feature branch. The branch was then pushed to a public fork of an open-source project we contribute to.

Detection

Our automated secret scanning tool (GitLeaks) detected the exposed credential within 3 minutes of the push.

Impact Assessment

What Was Exposed

- Datadog API key (logging service)
- No customer data was accessible via this credential
- Credential had read-only access to logging data

What Was NOT Exposed

- Customer data
- Production databases
- Authentication systems
- Other service credentials

Evidence of Exploitation

We reviewed: - Third-party access logs: No unauthorized access detected - Our application logs: No anomalies - Network traffic: No suspicious activity

Conclusion: No evidence of unauthorized access or data exfiltration.

Actions Taken

Immediate

1. Repository made private (3 minutes)
2. Exposed credential revoked (90 minutes)
3. New credentials generated and deployed (4 hours)
4. Git history scrubbed

Follow-Up

1. Enhanced pre-commit hooks deployed
2. Additional secret scanning rules added
3. Developer training scheduled
4. Repository access audit (in progress)

Affected Teams

Direct Impact

Team	Action Required	Deadline
Platform	Update Datadog API key	Complete
SRE	Verify monitoring restored	Complete

Informational

All engineering teams should: 1. Review your repositories for secrets 2. Ensure pre-commit hooks are active 3. Complete secret handling training

---

Lessons Learned

What Worked

- Automated secret scanning detected issue quickly
- Incident response process worked smoothly
- Vendor coordination was efficient
- No customer impact

What Needs Improvement

- Pre-commit hooks weren't enforced on all machines
- Public fork workflow needs clearer guidelines
- Secret scanning should block push, not just alert

Preventive Measures

Immediate (Complete)

1. **Enhanced pre-commit hooks**
   - Now blocks commits containing secrets
   - Mandatory for all engineers
2. **Secret scanning improvements**
   - Push blocking enabled
   - Additional patterns added
   - Faster alerting

Short-Term (This Quarter)

1. **Developer training**
   - Mandatory secret handling training
   - Due: July 31, 2024
2. **Repository audit**
   - Full scan of all repositories
   - Due: July 15, 2024
3. **Fork workflow documentation**
   - Clear guidelines for public contributions
   - Due: July 1, 2024

Long-Term

1. **Secret management improvements**
   - Reduce use of long-lived credentials
   - Implement dynamic secrets where possible
2. **Process improvements**
   - Automated compliance checking
   - Regular secret rotation

Required Actions by Role

All Engineers

- ☐ Verify pre-commit hooks installed: `pre-commit --version`
- ☐ Run local secret scan: `gitleaks detect`
- ☐ Complete training by July 31

Team Leads

- ☐ Ensure team members complete training
- ☐ Review team repositories for issues
- ☐ Update team workflows if needed

Security Champions

- ☐ Assist team with remediation
- ☐ Report any additional findings
- ☐ Attend debrief session

Resources

- Secret Handling Guide: [Internal Link]
- Pre-commit Hook Setup: [Internal Link]
- Training Registration: [Internal Link]
- Security Questions: #security-questions

Contact

For questions about this advisory: - Email: security@novatech.com - Slack: #security-questions - Urgent: #security-urgent

---

This advisory is for internal use only. Do not share externally.