Secret Rotation Runbook — 2026-04-20

Secret Rotation Runbook — 2026-04-20

Incident Summary

Date: 2026-04-20
Scope: 14 leaked credentials (git history exposure in two repositories)
Root Cause: Secrets echoed in CI logs, git-tracked config files, missing pre-commit hooks
Impact: No confirmed breach; rotation completed within 4 hours

Leaked Credentials

1. AWS IAM access keys (2x)
2. Azure Storage Account connection strings (3x)
3. BookStack API token
4. Slack webhook URLs (2x)
5. Cloudflare Access Client credentials (2x)
6. Bitwarden CLI session tokens (4x — expired)

Rotation Order (Critical ? Supporting)

1. **Bitwarden CLI unlock** — immediate session key rotation
2. **AWS IAM keys** — create new key, update config, delete old key
3. **Azure Storage Account keys** — regenerate key2 first (non-breaking), migrate scripts, regenerate key1
4. **Slack webhooks** — regenerate via Slack app settings
5. **Cloudflare Access** — rotate service tokens via Zero Trust dashboard

6. **BookStack API** — create new token, update ~/system/config/.bookstack-cred-cache.json, revoke old

Rotation Commands

```
# AWS IAM
aws iam create-access-key --user-name alai-admin --output json > /tmp/new-key.json
# Extract AccessKeyId and SecretAccessKey, update ~/.aws/credentials
aws iam delete-access-key --access-key-id OLD_KEY_ID --user-name alai-admin

# Azure Storage Account
az storage account keys renew --account-name alaibackups0ebb --key secondary
# Update ~/system/config/azure-backup.env with new key2 connection string
az storage account keys renew --account-name alaibackups0ebb --key primary

# Verification (test old credential returns 401/403)
curl -I https://alaibackups0ebb.blob.core.windows.net/system-db-backups \
  -H "x-ms-version: 2021-08-06" \
  -H "Authorization: Bearer OLD_TOKEN"
```

Lessons Learned

- **NEVER echo AWS IAM credentials:** `aws iam create-access-key` output must pipe to `jq` → Bitwarden immediately
- **Gitignore enforcement:** All files matching `*-cred-*`, `*.env`, `*-secret.*` → global gitignore + pre-commit hook
- **Hourly backup cron:** Add `gitleaks` scan before git bundle creation
- **Bitwarden item naming convention:** `ALAI — <service> — <context>` (Login type) for consistency

New Bitwarden Naming Convention

Format: `ALAI — <Service Name> — <Context>`
Type: Login (not Secure Note)
Examples:

- `ALAI — AWS IAM — alai-admin`
- `ALAI — Azure Storage — alaibackups0ebb`

- `ALAI — BookStack API — docs.basicconsulting.no`

Verification Protocol

```
# Test old credential fails (401/403)
curl -I <endpoint> -H "Authorization: Bearer OLD_TOKEN"

# Test new credential succeeds (200/204)
curl -I <endpoint> -H "Authorization: Bearer NEW_TOKEN"

# Update all config files
grep -r "OLD_TOKEN" ~/system/config/ ~/system/tools/
sed -i '' 's/OLD_TOKEN/NEW_TOKEN/g' ~/system/config/*.json
```

Next Incident Actions

1. Run `gitleaks detect --source ~/system/ --verbose` immediately
2. Prioritize rotation: IAM → Storage → API → Webhooks
3. Update Bitwarden with new credentials during rotation (not after)
4. Verify old credential invalidation with `curl 401` test
5. Document in BookStack within 24h

Revision #2
Created 2026-04-20 14:40:32 UTC by John
Updated 2026-05-31 20:06:10 UTC by John