Security Policy

Supported Versions

We actively support and provide security updates for the following versions:

Version	Supported
1.0.x	:white_check_mark:
< 1.0	:x:

Reporting a Vulnerability

We take security vulnerabilities seriously. If you discover a security vulnerability in this Ansible infrastructure repository, please report it responsibly.

How to Report

1. **DO NOT** create a public GitHub issue for security vulnerabilities
2. Send an email to: security@hanax.ai
3. Include the following information:
   - Description of the vulnerability
   - Steps to reproduce the issue
   - Potential impact assessment
   - Suggested fix (if available)

Response Timeline

- **Initial Response**: Within 24 hours of report
- **Assessment**: Within 72 hours
- **Fix Timeline**: Critical issues within 7 days, others within 30 days
- **Disclosure**: Coordinated disclosure after fix is deployed

Security Best Practices

This repository follows these security principles:

Infrastructure Security

- SSH host key verification enabled (`host_key_checking = True`)
- Vault password files excluded from version control
- Secrets managed through Ansible Vault
- Principle of least privilege for all access

Code Security

- All commits signed and verified
- Mandatory code review for security-related changes
- Automated security scanning in CI/CD pipeline
- Regular dependency updates and vulnerability scanning

Operational Security

- Production deployments require explicit confirmation
- Dry-run mode enabled by default for production targets
- Comprehensive logging and audit trails
- Regular security assessments and penetration testing

Security Contacts

- **Primary**: security@hanax.ai
- **Infrastructure Team**: infra@hanax.ai
- **Emergency**: +1-XXX-XXX-XXXX (24/7 on-call)

Acknowledgments

We appreciate responsible disclosure and will acknowledge security researchers who help improve our security posture.

Last updated: September 17, 2025