








name:  Security Issue
about: Report a security vulnerability or concern
title: '[SECURITY] '
labels: ['security', 'needs-triage', 'confidential']
assignees: ''

Security Issue

 **IMPORTANT:** If this is a critical security vulnerability that could be exploited, please report it privately through our security contact instead of creating a public issue.





Security Concern Type

- ☐  Critical vulnerability (immediate attention required)
- ☐  Security vulnerability (needs prompt attention)
- ☐  Security enhancement (improvement suggestion)
- ☐  Security audit finding
- ☐  Configuration security issue
- ☐  Security documentation gap

Affected Components

- ☐ Agent orchestration system
- ☐ Authentication/authorization
- ☐ Data storage/transmission
- ☐ API endpoints
- ☐ Configuration management
- ☐ Monitoring/logging
- ☐ CI/CD pipeline
- ☐ Infrastructure
- ☐ Documentation

Risk Assessment

- ☐  Critical (immediate system compromise possible)
- ☐  High (significant security impact)
- ☐  Medium (moderate security concern)
- ☐  Low (minor security improvement)

Vulnerability Details

Description

Attack Vector

Impact

- ☐ Data breach/exposure
- ☐ Unauthorized access
- ☐ System compromise
- ☐ Service disruption
- ☐ Privilege escalation
- ☐ Data manipulation
- ☐ Other: _____

Proof of Concept

Steps to demonstrate the issue:

- 1.
- 2.
- 3.

Environment Information

- **Component Version:** [e.g. v1.2.3]
- **Environment:** [e.g. production, staging, development]
- **Configuration:** [relevant configuration details]
- **Dependencies:** [relevant dependency versions]

Recommended Mitigation

Immediate Actions

- ☐ Action 1
- ☐ Action 2

Long-term Solutions

- ☐ Solution 1
- ☐ Solution 2





Workarounds

References

- [CVE Reference]
- [Security Advisory]
- [Documentation Link]



Confidentiality

- ☐  Highly confidential (restrict access)
- ☐  Confidential (limit distribution)
- ☐  Internal (team access)
- ☐  Public (can be discussed openly)



Additional Context

Related Security Issues

- Related to #
- Similar to #

Compliance Considerations

- ☐ SOC 2
- ☐ ISO 27001
- ☐ GDPR
- ☐ HIPAA
- ☐ PCI DSS
- ☐ Other: _____



Remediation Checklist

- ☐ Issue confirmed and reproduced
- ☐ Risk assessment completed
- ☐ Remediation plan developed
- ☐ Fix implemented
- ☐ Security testing completed
- ☐ Code review completed
- ☐ Documentation updated
- ☐ Security team approval
- ☐ Deployment to production
- ☐ Post-deployment verification

Severity:

CVSS Score:

Security Contact:

Note: This issue will be handled according to our security response procedures. Sensitive details may be moved to private channels as needed.