VIOE - Vulnerability Intelligence & Orchestration Engine

Change Log & Release Notes

Document Version: 1.0 **Classification:** Public **Last Updated:** January 2026

Table of Contents

1. Overview

1.1 Purpose

This document provides a comprehensive record of all VIOE releases, changes, and important information for users upgrading or evaluating the platform.

1.2 Versioning Scheme

VIOE follows semantic versioning: **MAJOR.MINOR.PATCH**

Component	Meaning	Example
MAJOR	Breaking changes, major features	1.0.0 → 2.0.0
MINOR	New features, backward compatible	1.0.0 → 1.1.0
PATCH	Bug fixes, minor improvements	1.0.0 → 1.0.1

1.3 Release Cadence

Release Type	Frequency
Major	Annual
Minor	Quarterly
Patch	Monthly
Security	As needed

1.4 Notification

Release notifications are distributed via:

- Email to account administrators
- In-app announcements
- Release notes in support portal
- Status page updates

---

2. Version History

2.1 Release Timeline

Version	Release Date	Type	Highlights
1.0.0	January 2026	Major	Initial Release

2.2 Support Status

Version	Status	Support End
1.0.x	Current	Active support

---

3. Release Notes - Version 1.0

3.1 Release Information

Attribute	Value
Version	1.0.0
Release Date	January 2026
Release Type	Major (Initial Release)
Stability	Production Ready

3.2 Executive Summary

VIOE 1.0 is the initial release of the Vulnerability Intelligence & Orchestration Engine, a comprehensive platform for enterprise vulnerability management powered by AI.

Key Value Propositions:

- AI-powered automatic team ownership assignment
- Intelligent noise reduction through suppression rules
- End-to-end remediation workflow orchestration
- Built-in compliance framework mapping
- Predictive threat intelligence

3.3 Feature Overview

Vulnerability Management

Feature	Description
Multi-Source Import	Import vulnerabilities from multiple scanners
Vulnerability Detail	Comprehensive view of each finding
Status Tracking	Full lifecycle management
SLA Management	Track remediation deadlines
Filtering & Search	Powerful filtering capabilities

Supported Severity Levels: Critical, High, Medium, Low, Info

Supported Status Values: Open, In Progress, Resolved, False Positive

AI-Powered Ownership

Feature	Description
Automatic Assignment	AI determines team ownership
Confidence Scoring	Transparency in assignment certainty
Multiple Data Sources	Git commits, CODEOWNERS, directory
Bulk Triage	Process multiple items at once
Ownership History	Complete audit trail

Confidence Levels: High (90%+), Medium (70-89%), Low (<70%)

Remediation Orchestration

Feature	Description
Task Management	Create and track remediation tasks
Jira Integration	Bidirectional sync with Jira
Policy Checks	Verify compliance with policies
Auto-Fix Suggestions	AI-generated fix recommendations
PR Workflow	Pull request creation support

Task Statuses: Todo, In Progress, In Review, Completed, Blocked

Asset Management

Feature	Description
Asset Inventory	Centralized asset registry
Risk Scoring	Automated risk calculation
Asset Types	Server, Workstation, Cloud, Database, Application
Environment Tracking	Production, Staging, Development

Team Management

Feature	Description
Team Creation	Define organizational teams
Performance Analytics	Team-level metrics
Slack Integration	Team channel notifications

Incident Response

Feature	Description
Incident Tracking	Full incident lifecycle
AI Assessment	Automated threat analysis
Containment Actions	Track mitigation activities
Timeline	Chronological event record
Reports	Incident documentation

Incident Statuses: Detected, Investigating, Containing, Resolved, Closed

Threat Intelligence

Feature	Description
Threat Hunting	Proactive threat detection
Predictive Analysis	30/60/90 day forecasting
Threat Modeling	STRIDE-based analysis
Threat Alerts	Detection notifications

Compliance & Reporting

Feature	Description
Framework Support	SOC 2, ISO 27001, GDPR, PCI DSS
Compliance Scoring	Framework alignment percentage
Gap Analysis	Non-compliance identification
Evidence Collection	Audit-ready documentation
Policy Recommendations	Suggested improvements

Dashboards & Analytics

Feature	Description
Main Dashboard	Key metrics and KPIs
Advanced Dashboard	Deep analytics
Trend Analysis	Time-series visualization
Team Analytics	Per-team metrics
Ownership Distribution	Confidence breakdown

Settings & Configuration

Feature	Description
Suppression Rules	Noise filtering configuration
AI Settings	Ownership assignment tuning
Integration Management	Scanner and tool connections
Notification Preferences	Alert configuration

3.4 Integrations

Scanner Integrations:

Scanner	Integration Type
Snyk	API / File Import
SonarQube	API / File Import
Checkmarx	API / File Import
Qualys	API / File Import
Tenable	API / File Import
Rapid7	API / File Import

Workflow Integrations:

Integration	Type
Jira	Bidirectional Sync
Slack	Notifications
Email	Alerts and Reports

Directory Integrations:

Integration	Type
Okta	SSO, User Mapping
Active Directory	Authentication, Groups

3.5 Technical Specifications

Specification	Details
Architecture	Single Page Application (React)
Backend	Base44 Platform
Database	PostgreSQL-compatible
Encryption	TLS 1.3, AES-256
Authentication	Session-based, MFA support
API	RESTful JSON API

Browser Support:

- Chrome (latest 2 versions)
- Firefox (latest 2 versions)
- Microsoft Edge (latest 2 versions)
- Safari (latest 2 versions)

3.6 System Requirements

Requirement	Specification
Browser	Modern browser with JavaScript
Internet	Stable connection required
Display	1280x720 minimum recommended

3.7 Bug Fixes

Not applicable - Initial release

3.8 Security Updates

Not applicable - Initial release with security built-in

Security Features Included:

- Role-based access control

- Audit logging
- Encryption at rest and in transit
- Session management
- MFA support

3.9 Impact Summary

Area	Impact
New Features	Full platform feature set
Data Migration	Not applicable (new)
API Changes	Initial API release
Breaking Changes	None
Required Action	Initial setup and configuration

---

4. Upgrade Instructions

4.1 Version 1.0 Installation

For New Deployments:

1. **Account Provisioning**
    - Contact sales or support for account creation
    - Receive initial administrator credentials
2. **Initial Configuration**
    - Log in as administrator
    - Complete initial setup wizard
    - Configure teams and users
3. **Integration Setup**
    - Connect vulnerability scanners
    - Configure Jira integration (if applicable)
    - Set up Slack notifications (if applicable)

4. **Data Import**
    - Import initial vulnerability scan data
    - Validate AI assignments
    - Configure suppression rules

4.2 Future Upgrade Guidelines

General Upgrade Process:

1. Review release notes for new version
2. Check for breaking changes
3. Test in staging environment (if available)
4. Schedule maintenance window
5. Execute upgrade
6. Validate functionality
7. Communicate to users

4.3 Configuration Backup

Before Any Upgrade:

- Export suppression rules
- Document integration settings
- Note custom configurations
- Verify backup is current

---

5. Deprecation Notices

5.1 Current Deprecations

No deprecations in initial release

5.2 Deprecation Policy

Phase	Notice	Action
Announced	Feature marked deprecated	Begin migration planning
Warning	6 months	Active warnings displayed
Disabled	12 months	Feature disabled
Removed	18 months	Code removed

5.3 Migration Guidance

Migration guidance will be provided for any deprecated features in future releases.

---

6. Known Issues

6.1 Current Known Issues

Issue ID	Description	Severity	Workaround	Status
VIOE-001	Large exports (>5000 items) may timeout	Medium	Use filters to reduce volume	Investigating
VIOE-002	Safari: Some chart tooltips display incorrectly	Low	Use Chrome or Firefox	Scheduled fix
VIOE-003	PDF import: Complex tables may not parse correctly	Low	Use CSV/JSON format	Under review

6.2 Issue Reporting

To report new issues:

1. Check if issue is known (this document)
2. Search knowledge base
3. Contact support with details

Information to Include:

- Steps to reproduce
- Expected vs. actual behavior

- Browser and OS information
- Screenshots if applicable

6.3 Issue Resolution

Known issues are tracked and prioritized based on:

- Severity
- Customer impact
- Workaround availability
- Development complexity

---

7. Upcoming Releases

7.1 Release Preview

The following represents current planning and is subject to change.

Version 1.1 (Planned - Next Quarter)

Feature	Description
Additional scanner integrations	Expand supported scanners
Custom report templates	User-defined report formats
Enhanced filtering	More filter options
Performance improvements	Faster dashboard loading

Version 1.2 (Planned - Future)

Feature	Description
Mobile application	iOS and Android support
Scheduled reports	Automatic report delivery
Advanced analytics	Additional charts and insights
API enhancements	New endpoints and capabilities

7.2 Feature Requests

To request features:

1. Submit through support portal
2. Contact Customer Success Manager
3. Participate in customer advisory programs

Feature requests are evaluated based on:

- Customer demand
- Strategic alignment
- Technical feasibility
- Resource availability

7.3 Beta Programs

Interested in early access to new features?

- Contact your Customer Success Manager
- Join our beta testing program
- Provide feedback on pre-release features

Appendix A: API Changes

A.1 Version 1.0 API

Base URL: `/api/v1`

Available Endpoints:

Endpoint	Methods	Description
`/vulnerabilities`	GET, POST, PATCH, DELETE	Vulnerability management
`/tasks`	GET, POST, PATCH, DELETE	Task management
`/assets`	GET, POST, PATCH, DELETE	Asset management
`/teams`	GET, POST, PATCH, DELETE	Team management
`/import`	POST	Data import
`/reports`	GET, POST	Report generation

A.2 Authentication

All API requests require authentication via Bearer token:

```
Authorization: Bearer <your-api-token>
```

A.3 Rate Limits

Limit	Value
Requests per minute	100
Requests per hour	1000

Appendix B: Database Schema Changes

B.1 Version 1.0 Schema

Initial schema - No migrations required

Core Tables:

- vulnerabilities
- remediation_tasks
- assets
- teams

- incidents
- threat_alerts
- compliance_reports
- suppression_rules
- ownership_logs

Appendix C: Configuration Changes

C.1 Version 1.0 Configuration

Default Settings:

Setting	Default Value
AI Confidence Threshold	70%
Session Timeout	30 minutes
Items Per Page	50
SLA - Critical	7 days
SLA - High	30 days
SLA - Medium	60 days
SLA - Low	90 days

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

Thank you for choosing VIOE. We're committed to continuous improvement.

VIOE - Vulnerability Intelligence & Orchestration Engine *Change Log & Release Notes*