



SECURITY ASSESSMENT

**Vision Industries, Inc.  
Oracle E-Business Suite R12  
Security Assessment Report**

January 31, 2016

## Table of Contents

<b>1 EXECUTIVE SUMMARY .....</b>	<b>2</b>		
<b>2 EXECUTIVE SUMMARY .....</b>	<b>3</b>		
Findings.....	3		
Configuration Assessment .....	3		
External Penetration Testing.....	3		
Additional Findings and Recommendations .....	4		
<b>3 SCOPE AND METHODOLOGY .....</b>	<b>5</b>		
Assessment Scope.....	5		
Technical Scope .....	6		
Application Modules .....	6		
Network Infrastructure .....	6		
Operating System .....	7		
Customizations.....	7		
Sarbanes-Oxley Compliance.....	8		
Timeline and Staffing .....	8		
Target Environment .....	8		
Methodology .....	8		
Vulnerability Information .....	9		
Complexity .....	9		
Remediation Effort.....	10		
Remediation Risk .....	10		
<b>4 ORACLE APPLICATIONS.....</b>	<b>11</b>		
4.1 Accounts and Passwords.....	11		
4.2 Default Application Accounts.....	12		
4.3 Application Passwords.....	13		
4.4 Application User Accounts .....	14		
4.5 Generic Application User Accounts .....	15		
4.6 Responsibilities.....	16		
4.6.1 Segregation of Duties for System Administration .....	16		
4.6.2 Responsibility Analysis .....	17		
4.7 Functional Security .....	17		
4.7.1 Menu Analysis .....	17		
4.7.2 Function Analysis .....	17		
4.8 User Profile Options.....	18		
4.8.1 Security Profile Options .....	18		
4.8.2 Auditing Profile Options.....	18		
4.8.3 Other Profile Options .....	19		
4.9 Auditing and Logging .....	19		
4.9.1 Applications Auditing.....	19		
4.9.2 Application Log files.....	20		
4.10 File Permissions.....	20		
4.11 Patches .....	21		
4.11.1 Oracle Critical Patch Updates.....	21		
4.11.2 Recommended Security Patches .....	22		
4.11.3 Other High Priority Patches .....	23		
<b>5 DATABASE ASSESSMENT .....</b>	<b>24</b>		
5.1 Accounts and Passwords.....	24		
5.1.1 Default Database Accounts .....	24		
5.1.2 Default Database Accounts Passwords.....	25		
5.1.3 Custom Database Accounts.....	26		
5.1.4 Database Account Password Analysis.....	26		
5.1.5 Custom Password Verification Function .....	27		
5.2 System and Object Privileges.....	28		
5.2.1 System Privileges .....	28		

5.2.2	Database Roles.....	29	8.2	Firewall Configuration.....	46
5.2.3	Object Privileges.....	29	8.2.1	Recommended Open Ports .....	46
5.3	Database Links.....	30	8.3	Application Firewall Configuration .....	47
5.4	Initialization Parameters.....	30	<b>9</b>	<b>CUSTOMIZATION ASSESSMENT .....</b>	<b>48</b>
5.5	File Permissions.....	31	9.1	Development Process.....	48
5.6	Security Patches .....	32	9.1.1	Coding Standards.....	48
5.6.1	Oracle Critical Patch Updates.....	32	9.1.2	Code Review Process.....	48
5.6.2	Other Database Security Patches .....	32	9.2	Change Management Process .....	49
5.7	Database Listener .....	32	9.3	Custom Database Objects.....	50
5.8	Auditing .....	33	9.4	Human Resources Interface.....	50
5.9	Logging .....	34	9.5	Order Entry Interface .....	51
<b>6</b>	<b>APPLICATION SERVER ASSESSMENT.....</b>	<b>36</b>	9.6	Other Interfaces.....	52
6.1	Apache .....	36	9.7	iSupplier Customizations.....	53
6.1.1	HTTPD Configuration Directives.....	36	9.7.1	SQL Injection.....	53
6.1.2	Logging.....	37	9.7.2	Cross Site Scripting (XSS).....	54
6.1.3	J2EE Configuration .....	38	9.7.3	Required Code Modifications .....	54
6.1.4	File Permissions .....	38	9.8	iStore Customizations .....	55
6.2	Forms Server .....	39	9.8.1	Authentication Issue.....	55
6.3	Reports Server .....	40	9.8.2	Item Security Bypass .....	56
6.4	Security Patches .....	41	9.8.3	Cross Site Scripting (XSS).....	57
6.4.1	Oracle Critical Patch Updates.....	41	9.8.4	Required Code Modifications .....	58
6.4.2	Other Security Patches.....	42	9.9	Self-Service Customizations .....	59
<b>7</b>	<b>OPERATING SYSTEM ASSESSMENT .....</b>	<b>43</b>	9.10	Custom Reports.....	60
7.1	User Accounts.....	43	<b>10</b>	<b>OPERATIONAL ASSESSMENT .....</b>	<b>61</b>
7.2	UNIX Security Patches.....	44	Summary .....	61	
7.3	Configuration .....	44	User Management (1.1) .....	62	
7.4	Auditing and Logging .....	45	Segregation of Duties (1.2) .....	63	
<b>8</b>	<b>NETWORK AND DMZ ASSESSMENT .....</b>	<b>46</b>	Database Security (1.3) .....	64	
8.1	Reverse Proxy Configuration .....	46	Network and Web Security (1.4) .....	65	
			Operating System Security (1.5).....	66	

Applications Auditing (2.1).....	67	Operating System Patching (5.4) .....	85
Database Auditing (2.2).....	68	Application Development (6.1).....	86
Web Logging (2.3) .....	69	Database Development (6.2).....	87
OS Auditing (2.4) .....	70	Web Development (6.3) .....	88
Application Monitoring and Troubleshooting (3.1) .....	71	Shell and File Transfer Development (6.4).....	89
Database Monitoring and Troubleshooting (3.2) .....	72	<b>11 ACTION ITEMS.....</b>	<b>90</b>
Web and Forms Monitoring and Troubleshooting (3.3) .....	73	11.1 Summary .....	90
Operating System Monitoring and Troubleshooting (3.4).....	75	11.2 Critical .....	91
Object Migrations (4.1).....	76	11.3 High Priority .....	92
Application Configuration Change Management (4.2).....	77	11.4 Low Priority .....	93
Database Change Control (4.3).....	78	11.5 Optional.....	94
Database Configuration Change Management (4.4).....	79	<b>12 APPENDICES .....</b>	<b>96</b>
Web Server Change Control (4.5) .....	80	<b>13 INDEX.....</b>	<b>103</b>
Operating System Change Control (4.6) .....	81		
Application Patching (5.1).....	82		
Database Patching (5.2).....	83		
Application Server Patching (5.3).....	84		