Vulnerability Type(s)	Publish Date	CVSS	Description CVE ID	Patch	NCIIPC ID
Application (A)					
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader Use Acrobat to convert, edit and sign PDF files at your desk or on the go; Adobe Acrobat DC is a trusted PDF creator; Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents.; Adobe Reader is the most popular program in the world for viewing, creating, managing and manipulating PDF (Portable Document Format) files.					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-10-21	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB-41116/01

			2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7853. **Reference: CVE-2016-7854**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-10-21	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB-41116/02

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7854. **Reference: CVE-2016-7853**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-10-21	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB-41116/03

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7853, and CVE-2016-7854. **Reference: CVE-2016-7852**		
Alien Vault					
Open Source Security Information And Event Management; Unified Security Management OSSIM, Alien Vault's Open Source Security Information and Event Management (SIEM) product, provides you with a feature-rich open source SIEM complete with event collection, normalization and correlation; Alien Vault Unified Security Management (USM) is an all-in-one platform designed and					

priced to ensure that mid-market organizations can effectively defend themselves against today's advanced threats.					
Cross Site Scripting	2016-10-28	4.3	Multiple GET parameters in the vulnerability scan scheduler of AlienVault OSSIM and USM before 5.3.2 are vulnerable to reflected XSS. **Reference: CVE-2016-8583**	https://www.alienvault.com/forums/discussion/7766/security-advisory-alienvault-5-3-2-address-70-vulnerabilities	A-ALI-OPEN - 41116/04
SQL Injection	2016-10-28	7.5	A vulnerability exists in gauge.php of AlienVault OSSIM and USM before 5.3.2 that allows an attacker to execute an arbitrary SQL query and retrieve database information or read local system files via MySQL's LOAD_FILE. **Reference: CVE-2016-8582**	https://www.alienvault.com/forums/discussion/7766/security-advisory-alienvault-5-3-2-address-70-vulnerabilities	A-ALI-OPEN - 41116/05
Cross Site Scripting	2016-10-28	4.3	A persistent XSS vulnerability exists in the User-Agent header of the login process of AlienVault OSSIM and USM before 5.3.2 that allows an attacker to steal session IDs of logged in users when the current sessions are viewed by an administrator. **Reference: CVE-2016-8581**	https://www.alienvault.com/forums/discussion/7766/security-advisory-alienvault-5-3-2-address-70-vulnerabilities	A-ALI-OPEN - 41116/06
Execute Code	2016-10-28	7.5	PHP object injection vulnerabilities exist in multiple widget files in AlienVault OSSIM and USM before 5.3.2. These vulnerabilities allow arbitrary PHP code	https://www.alienvault.com/forums/discussion/7766/security-advisory-alienvault-5-	A-ALI-OPEN - 41116/07

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			execution via magic methods in included classes. **Reference: CVE-2016-8580**	3-2-address-70-vulnerabilities	
Artifex					
Mujs MuJS is a lightweight Javascript interpreter designed for embedding in other software to extend them with scripting capabilities.					
Gain Information	2016-10-28	5	Artifex Software, Inc. MuJS before a5c747f1d40e8d6659a37a8d25f13fb5acf8e767 allows context-dependent attackers to obtain sensitive information by using the "opname in crafted JavaScript file" approach, related to an "Out-of-Bounds read" issue affecting the jsC_dumpfunction function in the jsdump.c component. **Reference: CVE-2016-9017**	http://bugs.ghostscript.com/show_bug.cgi?id=697171	A-ART-MUJS-41116/08
Denial of Service; Execute Code	2016-10-28	5	An out-of-bounds read vulnerability was observed in Sp_replace_regexp function of Artifex Software, Inc. MuJS before 5000749f5afe3b956fc916e407309de840997f4a. A successful exploitation of this issue can lead to code execution or denial of service condition. **Reference: CVE-2016-7506**	http://bugs.ghostscript.com/show_bug.cgi?id=697141	A-ART-MUJS-41116/09
Denial of Service; Execute Code; Overflow	2016-10-28	7.5	A buffer overflow vulnerability was observed in divby function of Artifex Software, Inc.	http://bugs.ghostscript.com/show_bug.cgi?id=69714	A-ART-MUJS-41116/10

			MuJS before 8c805b4eb19cf2af689c860b77e6111d2ee439d5. A successful exploitation of this issue can lead to code execution or denial of service condition. **Reference: CVE-2016-7505**	0	
Denial of Service; Execute Code	2016-10-28	7.5	A use-after-free vulnerability was observed in Rp_toString function of Artifex Software, Inc. MuJS before 5c337af4b3df80cf967e4f9f6a21522de84b392a. A successful exploitation of this issue can lead to code execution or denial of service condition. **Reference: CVE-2016-7504**	http://bugs.ghostscript.com/show_bug.cgi?id=697142	A-ART-MUJS-41116/11
Bitcoin Knots Project					
Bitcoin Knots Bitcoin Knots is a derivative of Bitcoin Core with a collection of improvements maintained out of the master git tree.					
NA	2016-10-28	2.1	In Bitcoin Knots v0.11.0.ljr20150711 through v0.13.0.knots20160814 (fixed in v0.13.1.knots20161027), the debug console stores sensitive information including private keys and the wallet passphrase in its persistent command history. **Reference: CVE-2016-8889**	https://bitcointalk.org/index.php?topic=1618462.0	A-BIT-BITCO-41116/12
Botan Project					
Botan Botan is a BSD-licensed cryptographic library written in C++.					
Gain	2016-10-28	2.1	In Botan 1.11.29 through	https://bota	A-BOT-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Information			1.11.32, RSA decryption with certain padding options had a detectable timing channel which could given sufficient queries be used to recover plaintext, aka an "OAEP side channel" attack. **Reference: CVE-2016-8871**	n.randombit.net/security.html	BOTAN-41116/13
Cisco					
Adaptive Security Appliance Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities.					
NA	2016-10-27	7.1	A vulnerability in the local Certificate Authority (CA) feature of Cisco ASA Software before 9.6(1.5) could allow an unauthenticated, remote attacker to cause a reload of the affected system. The vulnerability is due to improper handling of crafted packets during the enrollment operation. An attacker could exploit this vulnerability by sending a crafted enrollment request to the affected system. An exploit could allow the attacker to cause the reload of the affected system. Note: Only HTTPS packets directed to the Cisco ASA interface, where the local CA is allowing user enrollment, can be used to trigger this vulnerability. This vulnerability affects systems configured in routed firewall mode and in single or multiple	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-ca	A-CIS-ADAPT-41116/14

			context mode. **Reference: CVE-2016-6431**		
Email Security Appliance Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats.					
Denial of Service	2016-10-28	5	A vulnerability in local FTP to the Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition when the FTP application unexpectedly quits. More Information: CSCux68539. Known Affected Releases: 9.1.0-032 9.7.1-000. Known Fixed Releases: 9.1.1-038. **Reference: CVE-2016-6358**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa6	A-CIS-EMAIL-41116/15
Bypass	2016-10-28	5	A vulnerability in the configured security policies, including drop email filtering, in Cisco AsyncOS for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass a configured drop filter by using an email with a corrupted attachment. More Information: CSCuz01651. Known Affected Releases: 10.0.9-015 9.7.1-066 9.9.6-026. **Reference: CVE-2016-6357**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa5	A-CIS-EMAIL-41116/16
Denial of Service	2016-10-28	7.8	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances could	https://tools.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-EMAIL-41116/17

			allow an unauthenticated, remote attacker to cause an affected device to stop scanning and forwarding email messages due to a denial of service (DoS) condition. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to apply a message filter or content filter to incoming email attachments. The vulnerability is not limited to any specific rules or actions for a message filter or content filter. More Information: CSCuz63143. Known Affected Releases: 8.5.7-042 9.7.0-125. Known Fixed Releases: 10.0.0-125 9.1.1-038 9.7.2-047. **Reference: CVE-2016-6356**	visory/cisco-sa-20161026-esa3	
Denial of Service	2016-10-28	7.8	A vulnerability in the email attachment scanning functionality of the Advanced Malware Protection (AMP) feature of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to cause an affected device to stop scanning and forwarding email messages due to a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa2	A-CIS-EMAIL-41116/18

			denial of service (DoS) condition. Affected Products: This vulnerability affects Cisco AsyncOS Software releases 9.7.1 and later, prior to the first fixed release, for both virtual and hardware Cisco Email Security Appliances, if the AMP feature is configured to scan incoming email attachments. More Information: CSCuy99453. Known Affected Releases: 9.7.1-066. Known Fixed Releases: 10.0.0-125 9.7.1-207 9.7.2-047. **Reference: CVE-2016-1486**		
Denial of Service	2016-10-28	7.8	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to apply a message filter that contains certain rules. More Information: CSCux59873. Known Affected Releases: 8.5.6-106 9.1.0-032 9.7.0-125.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa1	A-CIS-EMAIL-41116/19

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Known Fixed Releases: 9.1.1-038 9.7.1-066. **Reference: CVE-2016-1481**		
Bypass	2016-10-28	5	A vulnerability in the Multipurpose Internet Mail Extensions (MIME) scanner of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) and Web Security Appliances (WSA) could allow an unauthenticated, remote attacker to bypass configured user filters on the device. Affected Products: all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco ESA and Cisco WSA, both virtual and hardware appliances, if the software is configured with message or content filters to scan incoming email attachments. More Information: CSCuw03606, CSCux59734. Known Affected Releases: 8.0.0-000 8.5.6-106 9.0.0-000 9.1.0-032 9.6.0-042 9.5.0-444 WSA10.0.0-000. Known Fixed Releases: 9.1.1-038 9.7.1-066. **Reference: CVE-2016-1480**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa1	A-CIS-EMAIL-41116/20
Cross Site Scripting	2016-10-28	4.3	A vulnerability in the display of email messages in the Messages in Quarantine (MIQ) view in Cisco AsyncOS for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-	A-CIS-EMAIL-41116/21

			attacker to cause a user to click a malicious link in the MIQ view. The malicious link could be used to facilitate a cross-site scripting (XSS) or HTML injection attack. More Information: CSCuz02235. Known Affected Releases: 8.0.2-069. Known Fixed Releases: 9.1.1-038 9.7.2-047. **Reference: CVE-2016-1423**	esa4	
Denial of Service	2016-10-28	5	A vulnerability in Advanced Malware Protection (AMP) for Cisco Email Security Appliances (ESA) and Web Security Appliances (WSA) could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition due to the AMP process unexpectedly restarting. Affected Products: Cisco AsyncOS Software for Email Security Appliances (ESA) versions 9.5 and later up to the first fixed release, Cisco AsyncOS Software for Web Security Appliances (WSA) all versions prior to the first fixed release. More Information: CSCux56406, CSCux59928. Known Affected Releases: 9.6.0-051 9.7.0-125 8.8.0-085 9.5.0-444 WSA10.0.0-000. Known Fixed Releases: 9.7.1-066 WSA10.0.0-233. **Reference: CVE-2016-**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa3	A-CIS-EMAIL-41116/22

			6360		
Email Security Appliance; Web Security Appliance; Web Security Appliance 8.0.5 Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats; Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes, integrated into one appliance.					
Bypass	2016-10-28	5	Vulnerability in the email message and content filtering for malformed Multipurpose Internet Mail Extensions (MIME) headers of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) and Web Security Appliances (WSA) could allow an unauthenticated, remote attacker to bypass the filtering functionality of the targeted device. Emails that should have been quarantined could instead be processed. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco ESA and Cisco WSA on both virtual and hardware appliances that are configured with message or content filters to scan incoming email attachments. More Information: CSCuy54740, CSCuy75174. Known Affected Releases: 9.7.1-066 9.5.0-575 WSA10.0.0-000. Known Fixed Releases: 10.0.0-125 9.1.1-038 9.7.2-047. **Reference: CVE-2016-6372**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa2	A-CIS-EMAIL-41116/23
Evolved Programmable Network Manager; Prime Infrastructure					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cisco Evolved Programmable Network Manager provides simplified, converged, multilayer management of carrier-grade networks of all sizes; Cisco Prime Infrastructure simplifies the management of wireless and wired networks. It offers Day 0 and 1 provisioning, as well as Day N assurance from the branch to the data center.					
SQL Injection	2016-10-27	6.5	Vulnerability in the Cisco Prime Infrastructure and Evolved Programmable Network Manager SQL database interface could allow an authenticated, remote attacker to impact system confidentiality by executing a subset of arbitrary SQL queries that can cause product instability. More Information: CSCva27038, CSCva28335. Known Affected Releases: 3.1(0.128), 1.2(400), 2.0(1.0.34A). **Reference: CVE-2016-6443**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-prime	A-CIS-EVOLV-41116/24
Finesse Cisco Finesse is a next-generation agent and supervisor desktop designed to improve the customer care experience your contact center delivers.					
Cross Site Request Forgery	2016-10-27	6.8	Vulnerability in Cisco Finesse Agent and Supervisor Desktop Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against the user of the web interface. More Information: CSCvb57213. Known Affected Releases: 11.0(1). **Reference: CVE-2016-6442**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-fin	A-CIS-FINES-41116/25
Firepower Management Center The Firepower Management Center analyzes your network's vulnerabilities, prioritizes any attacks, and recommends protections so your security team can focus on strategic activities.					
Denial of Service;	2016-10-27	4.3	A vulnerability in the detection engine	https://tools.cisco.com/se	A-CIS-FIREP-41116/26

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Bypass			reassembly of HTTP packets for Cisco Firepower System Software before 6.0.1 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to the Snort process unexpectedly restarting. The vulnerability is due to improper handling of an HTTP packet stream. An attacker could exploit this vulnerability by sending a crafted HTTP packet stream to the detection engine on the targeted device. An exploit could allow the attacker to cause a DoS condition if the Snort process restarts and traffic inspection is bypassed or traffic is dropped. **Reference: CVE-2016-6439**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-fpsnort	
Ip Interoperability And Collaboration System Cisco IP Interoperability and Collaboration System (IPICS) can simplify radio dispatch operations and improve response to incidents, emergencies, and facility events.					
NA	2016-10-28	10	A vulnerability in the inter device communications interface of the Cisco IP Interoperability and Collaboration System (IPICS) Universal Media Services (UMS) could allow an unauthenticated, remote attacker to modify configuration parameters of the UMS and cause the system to become unavailable. Affected Products: This vulnerability affects Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ipics	A-CIS-IPIN-41116/27

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			IPICS releases 4.8(1) to 4.10(1). More Information: CSCva46644. Known Affected Releases: 4.10(1) 4.8(1) 4.8(2) 4.9(1) 4.9(2). **Reference: CVE-2016-6397**		
Meeting Server Cisco Meeting Server brings video, audio, and web communication together to meet the collaboration needs of the modern workplace.					
Gain Information	2016-10-27	5	Vulnerability in Web Bridge for Cisco Meeting Server could allow an unauthenticated, remote attacker to retrieve memory from a connected server. More Information: CSCvb03308. Known Affected Releases: 1.8, 1.9, 2.0. **Reference: CVE-2016-6446**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms1	A-CIS-MEETI-41116/28
NA	2016-10-27	6.4	A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) service of the Cisco Meeting Server (CMS) before 2.0.6 and Acano Server before 1.8.18 and 1.9.x before 1.9.6 could allow an unauthenticated, remote attacker to masquerade as a legitimate user. This vulnerability is due to the XMPP service incorrectly processing a deprecated authentication scheme. A successful exploit could allow an attacker to access the system as another user. **Reference: CVE-2016-6445**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-msc	A-CIS-MEETI-41116/29

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cross Site Request Forgery	2016-10-27	6.8	A vulnerability in Cisco Meeting Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a Web Bridge user. More Information: CSCvb03308. Known Affected Releases: 1.8, 1.9, 2.0. **Reference: CVE-2016-6444**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms	A-CIS-MEETI-41116/30
Unified Communications Manager Cisco Unified Communications Manager is a unified communications call control platform that can deliver the right experience to the right endpoint.					
NA	2016-10-27	4.3	The Cisco Unified Communications Manager (CUCM) may be vulnerable to data that can be displayed inside an iframe within a web page, which in turn could lead to a clickjacking attack. More Information: CSCuz64683 CSCuz64698. Known Affected Releases: 11.0(1.10000.10), 11.5(1.10000.6), 11.5(0.99838.4). Known Fixed Releases: 11.0(1.22048.1), 11.5(0.98000.1070), 11.5(0.98000.284)11.5(0.98000.346), 11.5(0.98000.768), 11.5(1.10000.3), 11.5(1.10000.6), 11.5(2.10000.2). **Reference: CVE-2016-6440**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-ucm	A-CIS-UNIFI-41116/31
Wide Area Application Services Wide Area Application Services (WAAS) is a Cisco Systems technology that improves the performance of applications on a wide area network (WAN).					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	2016-10-27	7.1	A vulnerability in the SSL session cache management of Cisco Wide Area Application Services (WAAS) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to high consumption of disk space. The user would see a performance degradation. More Information: CSCva03095. Known Affected Releases: 5.3(5), 6.1(1), 6.2(1). Known Fixed Releases: 5.3(5g)1, 6.2(2.32). **Reference: CVE-2016-6437**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-waas	A-CIS-WIDE - 41116/32
Docker					
Docker Docker is an open-source project that automates the deployment of Linux applications inside software containers.					
Bypass	2016-10-28	5	Docker Engine 1.12.2 enabled ambient capabilities with misconfigured capability policies. This allowed malicious images to bypass user permissions to access files within the container filesystem or mounted volumes. **Reference: CVE-2016-8867**	https://www.docker.com/docker-cve-database	A-DOC-DOCKE-41116/33
Docker2aci Project					
Docker2aci docker2aci is a small library and CLI binary that converts Docker images to ACI.					
NA	2016-10-28	2.1	docker2aci <= 0.12.3 has an infinite loop when handling local images with cyclic dependency chain. **Reference: CVE-2016-**	https://github.com/appc/docker2aci/issues/203	A-DOC-DOCKE-41116/34

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			8579		
Dokuwiki					
Dokuwiki DokuWiki is a simple to use Wiki aimed at the documentation needs of a small company. It works on plain text files and thus needs no database.					
NA	2016-10-31	4.3	DokuWiki 2016-06-26a and older uses $_SERVER[HTTP_HOST] instead of the baseurl setting as part of the password-reset URL. This can lead to phishing attacks. (A remote unauthenticated attacker can change the URL's hostname via the HTTP Host header.) The vulnerability can be triggered only if the Host header is not part of the web server routing process (e.g., if several domains are served by the same web server). **Reference: CVE-2016-7965**	https://github.com/splitbrain/dokuwiki/issues/1709	A-DOK-DOKUW-41116/35
NA	2016-10-31	4.3	The sendRequest method in HTTPClient Class in file /inc/HTTPClient.php in DokuWiki 2016-06-26a and older, when media file fetching is enabled, has no way to restrict access to private networks. This allows users to scan ports of internal networks via SSRF, such as 10.0.0.1/8, 172.16.0.0/12, and 192.168.0.0/16. **Reference: CVE-2016-7964**	https://github.com/splitbrain/dokuwiki/issues/1708	A-DOK-DOKUW-41116/36
Dotcms					
dotCMS is an Open Source Content Management System (CMS), built on leading Java technology and open standards.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

NA	2016-10-28	5	In dotCMS 3.2.1, attacker can load captcha once, fill it with correct value and then this correct value is ok for forms with captcha check later. **Reference: CVE-2016-8600**	https://github.com/dotCMS/core/issues/9330	A-DOT-DOTCM-41116/37
Foxitsoftware					
Phantompdf; Reader Foxit PhantomPDF Standard provides you with a full suite of PDF viewing, sharing, and editing features, designed to make working with PDFs as convenient as possible; Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing.					
Denial of Service	2016-10-31	4.3	The thumbnail shell extension plugin (FoxitThumbnailHndlr_x86.dll) in Foxit Reader and PhantomPDF before 8.1 on Windows allows remote attackers to cause a denial of service (out-of-bounds write and application crash) via a crafted JPEG2000 image embedded in a PDF document, aka an "Exploitable - Heap Corruption" issue. **Reference: CVE-2016-8879**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-41116/38
Execute Code	2016-10-31	6.8	Out-of-Bounds read vulnerability in Foxit Reader and PhantomPDF before 8.1 on Windows, when the gflags app is enabled, allows remote attackers to execute arbitrary code via a crafted BMP image embedded in the XFA stream in a PDF document, aka "Data from Faulting Address may be used as a return value starting at	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-41116/39

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			FOXITREADER." **Reference: CVE-2016-8878**		
Exec Code Overflow	2016-10-31	6.8	Heap buffer overflow (Out-of-Bounds write) vulnerability in Foxit Reader and PhantomPDF before 8.1 on Windows allows remote attackers to execute arbitrary code via a crafted JPEG2000 image embedded in a PDF document, aka a "corrupted suffix pattern" issue. **Reference: CVE-2016-8877**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-41116/40
Execute Code	2016-10-31	6.8	Out-of-Bounds read vulnerability in Foxit Reader and PhantomPDF before 8.1 on Windows, when the gflags app is enabled, allows remote attackers to execute arbitrary code via a crafted TIFF image embedded in the XFA stream in a PDF document, aka "Read Access Violation starting at FoxitReader." **Reference: CVE-2016-8876**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-41116/41
Denial of Service	2016-10-31	4.3	The ConvertToPDF plugin in Foxit Reader and PhantomPDF before 8.1 on Windows, when the gflags app is enabled, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted TIFF image, aka "Data from Faulting Address is used as one or more arguments in a	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-41116/42

			subsequent Function Call starting at ConvertToPDF_x86!CreateFXPDFConvertor." **Reference: CVE-2016-8875**		
Reader Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing.					
Execute Code	2016-10-31	4.6	Foxit Reader for Mac 2.1.0.0804 and earlier and Foxit Reader for Linux 2.1.0.0805 and earlier suffered from a vulnerability where weak file permissions could be exploited by attackers to execute arbitrary code. After the installation, Foxit Reader's core files were world-writable by default, allowing an attacker to overwrite them with backdoor code, which when executed by privileged user would result in Privilege Escalation, Code Execution, or both. **Reference: CVE-2016-8856**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READE-41116/43
HP					
System Management Homepage The HPE System Management Homepage (SMH) is a web-based interface that consolidates and simplifies the management of ProLiant and Integrity servers running Microsoft Windows or Linux, or HPE 9000 and HPE Integrity servers running HP-UX 11i.					
Overflow	2016-10-28	7.8	HPE System Management Homepage before v7.6 allows remote attackers to have an unspecified impact via unknown vectors, related to a "Buffer Overflow" issue. **Reference: CVE-2016-4396**	https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05320149	A-HP-SYSTE-41116/44

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Overflow	2016-10-28	7.8	HPE System Management Homepage before v7.6 allows remote attackers to have an unspecified impact via unknown vectors, related to a "Buffer Overflow" issue. **Reference: CVE-2016-4395**	https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05320149	A-HP-SYSTE-41116/45
Gain Information	2016-10-28	5.8	HPE System Management Homepage before v7.6 allows remote attackers to obtain sensitive information via unspecified vectors, related to an "HSTS" issue. **Reference: CVE-2016-4394**	https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05320149	A-HP-SYSTE-41116/46
Cross Site Scripting; Gain Information	2016-10-28	3.5	HPE System Management Homepage before v7.6 allows "remote authenticated" attackers to obtain sensitive information via unspecified vectors, related to an "XSS" issue. **Reference: CVE-2016-4393**	https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05320149	A-HP-SYSTE-41116/47
Huge-it					
Catalog Huge-IT Product Catalog is made for demonstration, sale, and advertisements for your products.					
Cross Site Scripting	2016-10-21	6.5	SQLi and XSS in Huge IT catalog extension v1.0.4 for Joomla **Reference: CVE-2016-1000119**	NA	A-HUG-CATAL-41116/48
SQL Injection; Cross Site Scripting	2016-10-27	6.5	SQLi and XSS in Huge IT catalog extension v1.0.4 for Joomla **Reference: CVE-2016-1000120**	NA	A-HUG-CATAL-41116/49
Portfolio Gallery Manager Portfolio is perfect for creating various portfolios within various views. The product allows adding unlimited projects containing images, videos, description and titles for each portfolio.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SQL Injection; Cross Site Scripting	2016-10-21	6.5	Huge-IT Portfolio Gallery manager v1.1.5 SQL Injection and XSS **Reference: CVE-2016-1000116**	NA	A-HUG-PORTF-41116/50
SQL Injection; Cross Site Scripting	2016-10-21	6.5	Huge-IT Portfolio Gallery manager v1.1.5 SQL Injection and XSS **Reference: CVE-2016-1000115**	NA	A-HUG-PORTF-41116/51
Slider Huge IT Slider provides a quick and easy way to add custom sliders to WordPress websites (both to templates and posts/pages).					
SQL Injection; Cross Site Scripting	2016-10-27	6.5	XSS and SQLi in Huge IT Joomla Slider v1.0.9 extension **Reference: CVE-2016-1000122**	NA	A-HUG-SLIDE-41116/52
Cross Site Scripting	2016-10-27	3.5	XSS and SQLi in Huge IT Joomla Slider v1.0.9 extension **Reference: CVE-2016-1000121**	NA	A-HUG-SLIDE-41116/53
Cross Site Scripting	2016-10-21	6.5	XSS & SQLi in HugeIT slideshow v1.0.4 **Reference: CVE-2016-1000118**	NA	A-HUG-SLIDE-41116/54
Cross Site Scripting	2016-10-21	6.5	XSS & SQLi in HugeIT slideshow v1.0.4 **Reference: CVE-2016-1000117**	NA	A-HUG-SLIDE-41116/55
IBM					
Cloud Orchestrator IBM Cloud Orchestrator is a cloud management platform for automating provisioning of cloud services using policy-based tools.					
NA	2016-10-16	5.8	Open redirect vulnerability in IBM Cloud Orchestrator 2.4.x before 2.4.0 FP3 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	http://www-01.ibm.com/support/docview.wss?uid=swg2C1000124	A-IBM-CLOUD-41116/56

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-0204		
Financial Transaction Manager Financial Transaction Manager integrates, orchestrates and monitors financial transactions					
Cross Site Scripting	2016-10-28	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Financial Transaction Manager (FTM) for ACH Services 3.0.0.x before fp0015 and 3.0.1.0 before iFix0002 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5920**	http://www-01.ibm.com/support/docview.wss?uid=swg21989060	A-IBM-FINAN-41116/57
NA	2016-10-28	3.5	Payments Director in IBM Financial Transaction Manager (FTM) for ACH Services, Check Services, and Corporate Payment Services (CPS) 3.0.0.x before fp0015 and 3.0.1.0 before iFix0002 allows remote authenticated users to conduct clickjacking attacks via a crafted web site. **Reference: CVE-2016-3060**	http://www-01.ibm.com/support/docview.wss?uid=swg21989060	A-IBM-FINAN-41116/58
Rational Collaborative Lifecycle Management; Rational Quality Manager IBM Rational Collaborative Lifecycle Management is an application lifecycle management solution that includes IBM Rational Team Concert, IBM Rational DOORS Next Generation and IBM Rational Quality Manager products.					
Execute Code	2016-10-21	6.5	IBM Rational Quality Manager (RQM) and Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.x before 4.0.7 iFix11, 5.x before 5.0.2 iFix17, and 6.x before 6.0.1 ifix3 allow remote authenticated	http://www-01.ibm.com/support/docview.wss?uid=swg21989735	A-IBM-RATIO-41116/59

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			users to execute arbitrary OS commands via a crafted "HTML request." **Reference: CVE-2016-0326**		
Security Guardium IBM Security Guardium is a comprehensive data security platform that provides a full range of capabilities – from discovery and classification of sensitive data to vulnerability assessment to data and file activity monitoring to masking, encryption, blocking, alerting and quarantining to protect sensitive data.					
Execute Code; SQL Injection	2016-10-16	7.5	SQL injection vulnerability in IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-0249**	http://www-01.ibm.com/support/docview.wss?uid=swg21990363	A-IBM-SECUR-41116/60
Bypass; Gain Information	2016-10-21	2.1	IBM Security Guardium 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows local users to obtain sensitive cleartext information via unspecified vectors, as demonstrated by password information. **Reference: CVE-2016-0247**	http://www-01.ibm.com/support/docview.wss?uid=swg21990368	A-IBM-SECUR-41116/61
Cross Site Scripting	2016-10-21	4.3	Cross-site scripting (XSS) vulnerability in IBM Security Guardium 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-**	http://www-01.ibm.com/support/docview.wss?uid=swg21990377	A-IBM-SECUR-41116/62

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			0246		
Gain Information	2016-10-21	4	IBM Security Guardium 10.x through 10.1 before p100 allows remote authenticated users to obtain sensitive information by reading an Application Error message. **Reference: CVE-2016-0242**	http://www-01.ibm.com/support/docview.wss?uid=swg21990229	A-IBM-SECUR-41116/63
Security Guardium Database Activity Monitor IBM Security Guardium Data Activity Monitor prevents unauthorized data access, alerts on changes or leaks to help ensure data integrity, automates compliance controls and protects against internal and external threats.					
Execute Code	2016-10-21	7.2	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows local users to obtain administrator privileges for command execution via unspecified vectors. **Reference: CVE-2016-0328**	http://www-01.ibm.com/support/docview.wss?uid=swg21990226	A-IBM-SECUR-41116/64
NA	2016-10-21	6.5	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote authenticated users to spoof administrator accounts by sending a modified login request over HTTP. **Reference: CVE-2016-0241**	http://www-01.ibm.com/support/docview.wss?uid=swg21990219	A-IBM-SECUR-41116/65
Gain Information	2016-10-21	4.3	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700,	http://www-01.ibm.com/support/docview.wss?uid	A-IBM-SECUR-41116/66

			and 10.x through 10.1 before p100 does not enable the HSTS protection mechanism, which makes it easier for remote attackers to obtain sensitive information by leveraging use of HTTP. **Reference: CVE-2016-0240**	=swg21990232	
NA	2016-10-21	6.5	IBM Security Guardium Database Activity Monitor 9.x through 9.5 before p700 and 10.x through 10.0.1 before p100 allows remote authenticated users to make HTTP requests with administrator privileges via unspecified vectors. **Reference: CVE-2016-0239**	http://www-01.ibm.com/support/docview.wss?uid=swg21988999	A-IBM-SECUR-41116/67
Execute Code	2016-10-21	9	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote authenticated users to execute arbitrary commands with root privileges via the search field. **Reference: CVE-2016-0236**	http://www-01.ibm.com/support/docview.wss?uid=swg21990372	A-IBM-SECUR-41116/68
Websphere Application Server WebSphere Application Server (WAS) is a software product that performs the role of a web application server.					
Gain Information; Cross Site Request Forgery	2016-10-21	4	The Administrative Console in IBM WebSphere Application Server (WAS) 7.x before 7.0.0.43, 8.0.x before 8.0.0.13, and 8.5.x before 8.5.5.10 mishandles	http://www-01.ibm.com/support/docview.wss?uid=swg21980645	A-IBM-WEBSP-41116/69

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CSRFtoken cookies, which allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-0377**		
Iceni					
Argus Argus accurately converts the majority of PDF document types including financial/report based, newspaper/magazines, books and even structured PDF.					
Execute Code; Overflow	2016-10-28	6.8	An exploitable stack based buffer overflow vulnerability exists in the ipNameAdd functionality of Iceni Argus Version 6.6.04 (Sep 7 2012) NK - Linux x64 and Version 6.6.04 (Nov 14 2014) NK - Windows x64. A specially crafted pdf file can cause a buffer overflow resulting in arbitrary code execution. An attacker can send/provide malicious pdf file to trigger this vulnerability. **Reference: CVE-2016-8335**	http://www.talosintelligence.com/reports/2016-TALOS-0202/	A-ICE-ARGUS-41116/70
Execute Code; Overflow	2016-10-28	6.8	An exploitable stack-based buffer overflow vulnerability exists in the ipfSetColourStroke functionality of Iceni Argus version 6.6.04 A specially crafted pdf file can cause a buffer overflow resulting in arbitrary code execution. An attacker can provide a malicious pdf file to trigger this vulnerability. **Reference: CVE-2016-**	http://www.talosintelligence.com/reports/2016-TALOS-0200/	A-ICE-ARGUS-41116/71

			8333		
ISC					
Bind BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.					
Denial of Service	2016-10-21	5	ISC BIND 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via malformed options data in an OPT resource record. **Reference: CVE-2016-2848**	https://source.isc.org/cgi-bin/gitweb.cgi?p=bind9.git;a=commit;h=4adf97c32fcca7d00e5756607fd045f2aab9c3d4	A-ISC-BIND-41116/72
Libcsp Project					
Libcsp libcsp is a library that provides for C programmers a level of abstraction that makes programming with threads much easier.					
Execute Code; Overflow	2016-10-28	7.5	Buffer overflow in the zmq interface in csp_if_zmqhub.c in the libcsp library v1.4 and earlier allows hostile computers connected via a zmq interface to execute arbitrary code via a long packet. **Reference: CVE-2016-8598**	https://github.com/GomSpace/libcsp/pull/80	A-LIB-LIBCS-41116/73
Execute Code; Overflow	2016-10-28	7.5	Buffer overflow in the csp_sfp_recv_fp in csp_sfp.c in the libcsp library v1.4 and earlier allows hostile components with network access to the SFP underlying network layers to execute arbitrary code via specially crafted SFP packets. **Reference: CVE-2016-8597**	https://github.com/GomSpace/libcsp/pull/80	A-LIB-LIBCS-41116/74
Execute Code;	2016-10-28	7.5	Buffer overflow in the	https://githu	A-LIB-LIBCS-

Overflow			csp_can_process_frame in csp_if_can.c in the libcsp library v1.4 and earlier allows hostile components connected to the canbus to execute arbitrary code via a long csp packet. **Reference: CVE-2016-8596**	b.com/GomSpace/libcsp/pull/80	41116/75
Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
Execute Code	2016-10-28	6.8	An exploitable remote code execution vulnerability exists in the handling of TIFF images in LibTIFF version 4.0.6. A crafted TIFF document can lead to a type confusion vulnerability resulting in remote code execution. This vulnerability can be triggered via a TIFF file delivered to the application using LibTIFF's tag extension functionality. **Reference: CVE-2016-8331**	http://www.talosintelligence.com/reports/TALOS-2016-0190/	A-LIB-LIBTI-41116/76
Microfocus					
Rumba Ftp Rumba FTP is a graphical FTP client that combines ease-of-use with secured file transfer.					
Execute Code; Overflow	2016-10-27	6.8	Micro Focus Rumba FTP 4.X client buffer overflow makes it possible to corrupt the stack and allow arbitrary code execution. Fixed in: Rumba FTP 4.5 (HF 14668). This can only occur if a client connects to a malicious server. **Reference: CVE-2016-5764**	http://community.microfocus.com/microfocus/mainframe_solutions/rumba/w/knowledge_base/28731.rumba-ftp-4-x-security-update.aspx	A-MIC-RUMBA-41116/77

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Moodle					
Moodle Moodle is free and open-source software learning management system written in PHP and distributed under the GNU General Public License.					
SQL Injection; Gain Information	2016-10-28	5	** DISPUTED ** Moodle 3.1.2 allows remote attackers to obtain sensitive information via unspecified vectors, related to a "SQL Injection" issue affecting the Administration panel function in the installation process component. NOTE: the vendor disputes the relevance of this report, noting that "the person who is installing Moodle must know database access credentials and they can access the database directly; there is no need for them to create a SQL injection in one of the installation dialogue fields." **Reference: CVE-2016-7919**	NA	A-MOO-MOODL-41116/78
Novell					
Identity Manager Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.					
Cross Site Scripting	2016-10-27	4.3	XSS in NetIQ Designer for Identity Manager before 4.5.3 allows remote attackers to inject arbitrary HTML code via the nrfEntitlementReport.do CGI. **Reference: CVE-2016-1592**	https://download.novell.com/Download?buildid=QgHXVOxv310~	A-NOV-IDENT-41116/79

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cross Site Scripting	2016-10-27	4.3	XSS in NetIQ Designer for Identity Manager before 4.5.3 allows remote attackers to inject arbitrary HTML code via the accessMgrDN value of the forgotUser.do CGI. **Reference: CVE-2015-0787**	https://download.novell.com/Download?buildid=QgHXVOxv310~	A-NOV-IDENT-41116/80
Identity Manager; Identity Manager Identity Applications Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity; Application Identity Manager enables organizations to protect the data residing in business systems by eliminating hard coded and visible credentials.					
Cross Site Scripting	2016-10-27	3.5	XSS in NetIQ IDM 4.5 Identity Applications before 4.5.4 allows attackers able to change their username to inject arbitrary HTML code into the Role Assignment administrator HTML pages. **Reference: CVE-2016-1598**	https://download.novell.com/Download?buildid=xyswDCMsT7I~	A-NOV-IDENT-41116/81
Openjpeg					
Openjpeg OpenJPEG is an open-source JPEG 2000 codec written in C language.					
Execute Code; Overflow	2016-10-28	6.8	A buffer overflow in OpenJPEG 2.1.1 causes arbitrary code execution when parsing a crafted image. An exploitable code execution vulnerability exists in the jpeg2000 image file format parser as implemented in the OpenJpeg library. A specially crafted jpeg2000 file can cause an out of bound heap write resulting in heap corruption leading to	NA	A-OPE-OPENJ-41116/82

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			arbitrary code execution. For a successful attack, the target user needs to open a malicious jpeg2000 file. The jpeg2000 image file format is mostly used for embedding images inside PDF documents and the OpenJpeg library is used by a number of popular PDF renderers making PDF documents a likely attack vector. **Reference: CVE-2016-8332**		
NA	2016-10-29	5	Floating Point Exception (aka FPE or divide by zero) in opj_pi_next_cprl function in openjp2/pi.c:523 in OpenJPEG 2.1.2. **Reference: CVE-2016-9112**	https://github.com/uclouvain/openjpeg/issues/855	A-OPE-OPENJ-41116/83
Overflow	2016-10-30	5	Heap Buffer Overflow (WRITE of size 4) in function pnmtoimage of convert.c:1719 in OpenJPEG 2.1.2. **Reference: CVE-2016-9118**	https://github.com/uclouvain/openjpeg/issues/861	A-OPE-OPENJ-41116/84
Denial of Service	2016-10-30	4.3	NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a crafted j2k file. **Reference: CVE-2016-9117**	https://github.com/uclouvain/openjpeg/issues/860	A-OPE-OPENJ-41116/85
Denial of Service	2016-10-30	4.3	NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a	https://github.com/uclouvain/openjpeg/issues/859	A-OPE-OPENJ-41116/86

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			crafted j2k file. **Reference: CVE-2016-9116**		
Denial of Service;Overflow	2016-10-30	4.3	Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a crafted j2k file. **Reference: CVE-2016-9115**	https://github.com/uclouvain/openjpeg/issues/858	A-OPE-OPENJ-41116/87
Denial of Service	2016-10-30	5	There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG 2.1.2. image->comps[compno].data is not assigned a value after initialization(NULL). Impact is Denial of Service. **Reference: CVE-2016-9114**	https://github.com/uclouvain/openjpeg/issues/857	A-OPE-OPENJ-41116/88
Denial of Service	2016-10-30	5	There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJPEG 2.1.2. image->comps[0].data is not assigned a value after initialization(NULL). Impact is Denial of Service. **Reference: CVE-2016-9113**	https://github.com/uclouvain/openjpeg/issues/856	A-OPE-OPENJ-41116/89
Oracle					
Advanced Pricing The pricing engine is a software component of Oracle Advanced Pricing that is called by an application such as Oracle Order Management or iStore to apply pricing actions to transactions.					
NA	2016-10-25	5.8	Unspecified vulnerability in the Oracle Advanced Pricing component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-	A-ORA-ADVAN-41116/90

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			allows remote attackers to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5557**	2881722.html	
Advanced Supply Chain Planning Oracle Advanced Supply Chain Planning provides you with the option of using demands from all planned orders during hub and spoke planning. When you use your plans as demand schedules to other plans, the planning engine considers all planned orders in the source plan as demands and explodes down the bills of material creating demands for the lower level components.					
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Advanced Supply Chain Planning component in Oracle Supply Chain Products Suite 12.2.3 through 12.2.5 allows remote attackers to affect confidentiality and integrity via vectors related to MscObieeSrvlt. **Reference: CVE-2016-5599**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-ADVAN-41116/91
Agile Engineering Data Management Agile Engineering Data Management (e6) comprehensively supports all product-related enterprise processes for organizations in industrial manufacturing sectors.					
NA	2016-10-25	6.8	Unspecified vulnerability in the Oracle Agile Engineering Data Management component in Oracle Supply Chain Products Suite 6.1.3.0 and 6.2.0.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to webfileservices. **Reference: CVE-2016-5518**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/92
Agile Product Lifecycle Management Framework The integration between Agile PLM and Oracle E-Business Suite is designed to enable the product development process and address the primary use cases around the synchronization of product content information between Agile Product Collaboration and Oracle Manufacturing. This allows for					

rapid implementation of Oracle's next-generation integrated enterprise PLM processes helping the customers reduce costs and any risks associated with typical third-party and custom integrations.					
NA	2016-10-25	4.3	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality via unknown vectors, a different vulnerability than CVE-2016-5524. **Reference: CVE-2016-5527**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/93
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Apache Tomcat. **Reference: CVE-2016-5526**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/94
Gain Information	2016-10-25	5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality via unknown vectors, a different vulnerability than CVE-2016-5527. **Reference: CVE-2016-5524**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/95
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/96

			affect confidentiality, integrity, and availability via vectors related to AutoVue Java Applet. **Reference: CVE-2016-5523**		
Gain Information	2016-10-25	4	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect confidentiality via unknown vectors. **Reference: CVE-2016-5522**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/97
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5512. **Reference: CVE-2016-5521**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/98
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to RMIServlet. **Reference: CVE-2016-5515**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/99
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Agile PLM	http://www.oracle.com/tec	A-ORA-AGILE-41116/100

			component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to ExportServlet. **Reference: CVE-2016-5514**	hnetwork/security-advisory/cpuoct2016-2881722.html	
Gain Information	2016-10-25	4	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect confidentiality via vectors related to File Manager. **Reference: CVE-2016-5513**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/101
Cross Site Scripting	2016-10-25	4.3	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5521. **Reference: CVE-2016-5512**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/102
Gain Information	2016-10-25	5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality via unknown vectors. **Reference: CVE-2016-**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/103

			5510		
Gain Information	2016-10-25	4.7	Unspecified vulnerability in the Oracle Agile Product Lifecycle Management for Process component in Oracle Supply Chain Products Suite 6.1.0.4, 6.1.1.6, and 6.2.0.0 allows local users to affect confidentiality via vectors related to Supplier Portal. **Reference: CVE-2016-5504**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-AGILE-41116/104
Applications Dba Oracle Applications DBA is very different from a regular Oracle database administrator and requires specialized skills in business administration and Oracle application server architectures.					
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle Applications DBA component in Oracle E-Business Suite 12.1.3 and 12.2.3 through 12.2.6 allows remote administrators to affect confidentiality and integrity via vectors related to AD Utilities, a different vulnerability than CVE-2016-5567. **Reference: CVE-2016-5571**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-APPLI-41116/105
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle Applications DBA component in Oracle E-Business Suite 12.2.3 through 12.2.6 allows remote administrators to affect confidentiality and integrity via vectors related to AD Utilities. **Reference: CVE-2016-5570**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-APPLI-41116/106
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle Applications	http://www.oracle.com/tec	A-ORA-APPLI-41116/107

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			DBA component in Oracle E-Business Suite 12.1.3 and 12.2.3 through 12.2.6 allows remote administrators to affect confidentiality and integrity via vectors related to AD Utilities, a different vulnerability than CVE-2016-5571. **Reference: CVE-2016-5567**	hnetwork/security-advisory/cpuoct2016-2881722.html	
NA	2016-10-25	2.1	Unspecified vulnerability in the Oracle Applications DBA component in Oracle E-Business Suite 12.1.3 allows local users to affect confidentiality via vectors related to AD Utilities. **Reference: CVE-2016-5517**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-APPLI-41116/108
Business Intelligence Publisher Business Intelligence Publisher is the reporting solution to author, manage, and deliver all your reports and documents easier and faster than traditional reporting tools.					
Gain Information	2016-10-25	4	Unspecified vulnerability in the BI Publisher (formerly XML Publisher) component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, and 12.2.1.0.0 allows remote authenticated users to affect confidentiality via unknown vectors. **Reference: CVE-2016-3473**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-BUSIN-41116/109
Commerce Guided Search Oracle Commerce Guided Search and Oracle Commerce Experience Manager are the most effective way for your customers to dynamically explore your site and find relevant and desired items quickly					
NA	2016-10-25	5.8	Unspecified vulnerability in the Oracle Commerce Guided Search component in Oracle Commerce 6.2.2, 6.3.0,	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-COMME-41116/110

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6.4.1.2, and 6.5.0 through 6.5.2 allows remote attackers to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5482**	oct2016-2881722.html	
Commerce Service Center Commerce Service Center (CSC) is a customer service application that allows companies using Commerce to perform agent tasks such as managing customer profiles; creating and managing orders; issuing refunds and exchanges; processing returned items; and researching customer activity.					
NA	2016-10-25	5.8	Unspecified vulnerability in the Oracle Commerce Service Center component in Oracle Commerce 10.0.3.5 and 10.2.0.5 allows remote attackers to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5491**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-COMME-41116/111
NA	2016-10-25	5	Unspecified vulnerability in the Oracle Common Applications Calendar component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote attackers to affect confidentiality via vectors related to Resources Module. **Reference: CVE-2016-5575**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-COMMO-41116/112
Customer Interaction History Oracle Customer Interaction History provides applications with a common framework for capturing and accessing all "interaction" data associated with customer contacts. Oracle Customer Interaction History acts as a central repository and provides a consistent framework for tracking all automated or agent-based customer interactions.					
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Customer Interaction History	http://www.oracle.com/technetwork/sec	A-ORA-CUSTO-41116/113

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5592. **Reference: CVE-2016-5595**	urity-advisory/cpuoct2016-2881722.html	
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Customer Interaction History component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5587 and CVE-2016-5591. **Reference: CVE-2016-5593**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-CUSTO-41116/114
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Customer Interaction History component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5595. **Reference: CVE-2016-5592**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-CUSTO-41116/115
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Customer	http://www.oracle.com/tec	A-ORA-CUSTO-41116/116

			Interaction History component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5587 and CVE-2016-5593. **Reference: CVE-2016-5591**	hnetwork/security-advisory/cpuoct2016-2881722.html	
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Customer Interaction History component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5591 and CVE-2016-5593. **Reference: CVE-2016-5587**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-CUSTO-41116/117
Customer Relationship Management Technical Foundation Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers, assisting in customer retention and driving sales growth.					
Gain Information	2016-10-25	4	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote authenticated users to affect confidentiality via	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-CUSTO-41116/118

			unknown vectors. **Reference: CVE-2016-5596**		
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote attackers to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5589**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-CUSTO-41116/119
Data Integrator Oracle Data Integrator is a comprehensive data integration platform that covers all data integration requirements: from high-volume, high-performance batch loads, to event-driven, trickle-feed integration processes, to SOA-enabled data services.					
Gain Information	2016-10-25	3.5	Unspecified vulnerability in the Oracle Data Integrator component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, 12.1.2.0.0, 12.1.3.0.0, 12.2.1.0.0, and 12.2.1.1.0 allows remote authenticated users to affect confidentiality via vectors related to Code Generation Engine. **Reference: CVE-2016-5618**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATA - 41116/120
Gain Information	2016-10-25	3.5	Unspecified vulnerability in the Oracle Data Integrator component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.0.0, and 12.2.1.1.0 allows remote authenticated users to affect confidentiality via vectors related to Code	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATA - 41116/121

			Generation Engine. **Reference: CVE-2016-5602**		
Database An Oracle database is a collection of data treated as a unit. The purpose of a database is to store and retrieve related information.					
NA	2016-10-25	4.4	Unspecified vulnerability in the Kernel PDB component in Oracle Database Server 12.1.0.2 allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5572**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/122
NA	2016-10-25	4.4	Unspecified vulnerability in the RDBMS Security component in Oracle Database Server 12.1.0.2 allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5497**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/123
Database Server An Oracle database is a collection of data treated as a unit. The purpose of a database is to store and retrieve related information. A database server is the key to solving the problems of information management.					
NA	2016-10-25	6.5	Unspecified vulnerability in the OJVM component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows remote administrators to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5555**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/124
NA	2016-10-25	4.7	Unspecified vulnerability in the Kernel PDB component in Oracle Database Server 12.1.0.2	http://www.oracle.com/technetwork/security-	A-ORA-DATAB-41116/125

			allows local users to affect availability via unknown vectors. **Reference: CVE-2016-5516**	advisory/cpuoct2016-2881722.html	
Gain Information	2016-10-25	2.1	Unspecified vulnerability in the RDBMS Programmable Interface component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows local users to affect confidentiality via unknown vectors. **Reference: CVE-2016-5505**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/126
NA	2016-10-25	2.1	Unspecified vulnerability in the RDBMS Security component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows local users to affect confidentiality via unknown vectors, a different vulnerability than CVE-2016-5498. **Reference: CVE-2016-5499**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/127
Gain Information	2016-10-25	2.1	Unspecified vulnerability in the RDBMS Security component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows local users to affect confidentiality via unknown vectors, a different vulnerability than CVE-2016-5499. **Reference: CVE-2016-5498**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DATAB-41116/128
Gain Information	2016-10-25	4.3	Unspecified vulnerability in the RDBMS Security and SQL*Plus components in Oracle Database Server 11.2.0.4	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-DATAB-41116/129

			and 12.1.0.2 allows remote administrators to affect confidentiality via vectors related to DBA. **Reference: CVE-2016-3562**	oct2016-2881722.html	
Discoverer Discoverer is an intuitive ad-hoc query, reporting, analysis, and Web-publishing tool that empower business users at all levels of the organization to gain immediate access to information from data marts, data warehouses, online transaction processing systems and Oracle E-Business Suite.					
Gain Information	2016-10-25	5	Unspecified vulnerability in the Oracle Discoverer component in Oracle Fusion Middleware 11.1.1.7.0 allows remote attackers to affect confidentiality via vectors related to Viewer. **Reference: CVE-2016-5500**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DISCO-41116/130
NA	2016-10-25	5	Unspecified vulnerability in the Oracle Discoverer component in Oracle Fusion Middleware 11.1.1.7.0 allows remote attackers to affect confidentiality via vectors related to EUL Code & Schema. **Reference: CVE-2016-5495**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-DISCO-41116/131
Email Center Email Center Pro is a hosted email management solution that makes it easy to manage shared email accounts and group inboxes like info@yourcompany.com.					
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Email Center component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote attackers to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-EMAIL-41116/132

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			5586		
Enterprise Manager Base Platform Oracle Enterprise Manager is Oracle's on-premises management platform, providing a single pane of glass for managing all of a customer's Oracle deployments, whether in their data centers or in the Oracle Cloud.					
NA	2016-10-25	3.3	Unspecified vulnerability in the Enterprise Manager Base Platform component in Oracle Enterprise Manager Grid Control 12.1.0.5 allows local users to affect confidentiality and integrity via vectors related to Security Framework. **Reference: CVE-2016-5604**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-ENTER-41116/133
Flexcube Enterprise Limits And Collateral Management Oracle FLEXCUBE Enterprise Limits and Collateral Management integrates with your existing IT application landscape and offers you a single source for managing online, real-time exposure across the enterprise. Its process-centric architecture enables centralized collateral management, enterprise-wide limits definition, and tracking for effective exposure management as well as resource utilization.					
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component in Oracle Financial Services Applications 12.0.0 and 12.1.0 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5569**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/134
NA	2016-10-25	5.8	Unspecified vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component in Oracle Financial Services Applications 12.0.0 and	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/135

			12.1.0 allows remote attackers to affect confidentiality and integrity via vectors related to INFRA. **Reference: CVE-2016-5543**		
Flexcube Private Banking Oracle FLEXCUBE Private Banking Manage the Entire Wealth Management Business Cycle Plan, record, track, and manage a customer's wealth across a range of asset classes and instruments to deliver increased financial advisor productivity and improved customer relationships.					
NA	2016-10-25	4.9	Unspecified vulnerability in the Oracle FLEXCUBE Private Banking component in Oracle Financial Services Applications 12.0.1 through 12.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5493**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/136
Flexcube Universal Banking Oracle FLEXCUBE Universal Banking is a real-time, online, comprehensive approach to core banking requirements around the world, covering retail, corporate and investment banking functions. Oracle FLEXCUBE Universal Banking enables customers to be more agile by implementing business process-driven operations, reducing product time-to-market, and providing services that are customized with tight controls and risk management.					
NA	2016-10-25	7.8	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote attackers to affect confidentiality and integrity via vectors related to INFRA. **Reference: CVE-2016-5622**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/137

NA	2016-10-25	4	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 and 12.0.3, 12.1.0, and 12.2.0 allows remote authenticated users to affect confidentiality via vectors related to INFRA, a different vulnerability than CVE-2016-5603. **Reference: CVE-2016-5621**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/138
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote authenticated users to affect confidentiality and integrity via vectors related to INFRA, a different vulnerability than CVE-2016-5619. **Reference: CVE-2016-5620**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/139
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote authenticated users to affect confidentiality and integrity via vectors	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/140

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			related to INFRA, a different vulnerability than CVE-2016-5620. **Reference: CVE-2016-5619**		
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to INFRA. **Reference: CVE-2016-5607**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/141
Gain Information	2016-10-25	4	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote authenticated users to affect confidentiality via vectors related to INFRA, a different vulnerability than CVE-2016-5621. **Reference: CVE-2016-5603**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/142
NA	2016-10-25	4	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, and 12.0.1 through 12.0.3 allows	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/143

			remote authenticated users to affect confidentiality via vectors related to INFRA. **Reference: CVE-2016-5594**		
NA	2016-10-25	5.5	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3 allows remote authenticated users to affect confidentiality and integrity via vectors related to INFRA. **Reference: CVE-2016-5502**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/144
NA	2016-10-25	2.1	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.4.0 allows local users to affect confidentiality via vectors related to INFRA. **Reference: CVE-2016-5490**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/145
Gain Information	2016-10-25	4	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, and 12.0.1 allows remote authenticated users to affect confidentiality via vectors related to INFRA. **Reference: CVE-2016-5479**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-FLEXC-41116/146

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Glassfish Server GlassFish is an open-source application server project started by Sun Microsystems for the Java EE platform and now sponsored by Oracle Corporation.					
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle GlassFish Server component in Oracle Fusion Middleware 2.1.1, 3.0.1, and 3.1.2 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to Java Server Faces. **Reference: CVE-2016-5519**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-GLASS-41116/147
Hospitality Opera 5 Property Services Oracle Hospitality OPERA Property provides a full-featured, property-management system that enables you to deliver world-class guest service and increase operational efficiency across the property.					
NA	2016-10-25	4	Unspecified vulnerability in the Oracle Hospitality OPERA 5 Property Services component in Oracle Hospitality Applications 5.4.0.0 through 5.4.3.0, 5.5.0.0, and 5.5.1.0 allows remote authenticated users to affect confidentiality via vectors related to OPERA. **Reference: CVE-2016-5565**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-HOSPI-41116/148
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Hospitality OPERA 5 Property Services component in Oracle Hospitality Applications 5.4.0.0 through 5.4.3.0, 5.5.0.0, and 5.5.1.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-HOSPI-41116/149

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			OPERA. **Reference: CVE-2016-5564**		
NA	2016-10-25	6	Unspecified vulnerability in the Oracle Hospitality OPERA 5 Property Services component in Oracle Hospitality Applications 5.4.0.0 through 5.4.3.0, 5.5.0.0, and 5.5.1.0 allows remote administrators to affect confidentiality, integrity, and availability via vectors related to OPERA. **Reference: CVE-2016-5563**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-HOSPI-41116/150
Identity Manager Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.					
NA	2016-10-25	3.3	Unspecified vulnerability in the Oracle Identity Manager component in Oracle Fusion Middleware allows local users to affect confidentiality and integrity via vectors related to App Server. **Reference: CVE-2016-5506**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-IDENT-41116/151
Interaction Center Intelligence Oracle Interaction Center Intelligence (ICI) is an operational performance-management application for Oracle Interaction Centers.					
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle Interaction Center Intelligence component in Oracle E-Business Suite 12.1.1 through 12.1.3 allows remote attackers to affect confidentiality and integrity via unknown vectors.	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-INTER-41116/152

			Reference: CVE-2016-5585		
Iprocurement Oracle iProcurement is part of Oracle Applications, an integrated suite of E-Business solutions designed to transform your business into an E-Business.					
NA	2016-10-25	4.9	Unspecified vulnerability in the Oracle iProcurement component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5562**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-IPROC-41116/153
NA	2016-10-25	4.6	Unspecified vulnerability in the Oracle iRecruitment component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5581**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-IRECR-41116/154
Istore Oracle iStore is a powerful tool that allows businesses to create and manage online e-commerce sites.					
NA	2016-10-25	7.8	Unspecified vulnerability in the Oracle iStore component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via vectors related to Runtime Catalog. **Reference: CVE-2016-5489**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-ISTOR-41116/155

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

JDK;JRE

The Java Development Kit (JDK) is an implementation of either one of the Java Platform, Standard Edition; Java Platform, Enterprise Edition or Java Platform, Micro Edition platforms released by Oracle Corporation in the form of a binary product aimed at Java developers on Solaris, Linux, Mac OS X or Windows; Java Runtime Environment (JRE) is a software package that contains what is required to run a Java program. It includes a Java Virtual Machine implementation together with an implementation of the Java Class Library.

Gain Information	2016-10-25	4.3	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality via vectors related to Networking. **Reference: CVE-2016-5597**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/156
NA	2016-10-25	9.3	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5573. **Reference: CVE-2016-5582**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/157
NA	2016-10-25	6.8	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5582. **Reference: CVE-2016-5573**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/158
NA	2016-10-25	9.3	Unspecified vulnerability in Oracle Java SE 6u121,	http://www.oracle.com/tec	A-ORA-JDK;J-41116/159

			7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. **Reference: CVE-2016-5568**	hnetwork/security-advisory/cpuoct2016-2881722.html	
NA	2016-10-25	9.3	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D. **Reference: CVE-2016-5556**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/160
NA	2016-10-25	4.3	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to JMX. **Reference: CVE-2016-5554**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/161
NA	2016-10-25	4.3	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to Libraries. **Reference: CVE-2016-5542**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-JDK;J-41116/162
Micros Xstore Payment					
NA	2016-10-25	3.3	Unspecified vulnerability in the Oracle Retail Xstore Payment component in Oracle Retail Applications 1.x allows local users to affect confidentiality and integrity via unknown	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MICRO-41116/163

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			vectors. **Reference: CVE-2016-5540**		
NA	2016-10-25	4.6	Unspecified vulnerability in the Oracle Retail Xstore Payment component in Oracle Retail Applications 1.x allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5539**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MICRO-41116/164
Mysql MySQL is the most popular Open Source Relational SQL database management system. MySQL is one of the best RDBMS being used for developing web-based software applications.					
NA	2016-10-25	3.5	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-5633. **Reference: CVE-2016-8290**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/165
NA	2016-10-25	3.3	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows local users to affect integrity and availability via vectors related to Server: InnoDB. **Reference: CVE-2016-8289**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/166
NA	2016-10-25	4.9	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect integrity via vectors related to Server: InnoDB Plugin.	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/167

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-8288		
NA	2016-10-25	3.5	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Replication. **Reference: CVE-2016-8287**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/168
Gain Information	2016-10-25	3.5	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote authenticated users to affect confidentiality via vectors related to Server: Security: Privileges. **Reference: CVE-2016-8286**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/169
NA	2016-10-25	1.2	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows local users to affect availability via vectors related to Server: Replication. **Reference: CVE-2016-8284**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/170
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Types. **Reference: CVE-2016-8283**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/171
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-MYSQL-41116/172

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			related to Server: Security: Audit. **Reference: CVE-2016-5635**	oct2016-2881722.html	
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to RBR. **Reference: CVE-2016-5634**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/173
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-8290. **Reference: CVE-2016-5633**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/174
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer. **Reference: CVE-2016-5632**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/175
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Memcached. **Reference: CVE-2016-5631**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/176
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote	http://www.oracle.com/technetwork/security-	A-ORA-MYSQL-41116/177

			administrators to affect availability via vectors related to Server: InnoDB. **Reference: CVE-2016-5630**	advisory/cpuoct2016-2881722.html	
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Federated. **Reference: CVE-2016-5629**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/178
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: DML. **Reference: CVE-2016-5628**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/179
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to Server: InnoDB. **Reference: CVE-2016-5627**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/180
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS. **Reference: CVE-2016-5626**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/181

NA	2016-10-25	4.4	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Packaging. **Reference: CVE-2016-5625**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/182
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier allows remote authenticated users to affect availability via vectors related to DML. **Reference: CVE-2016-5624**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/183
NA	2016-10-25	4.4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Error Handling. **Reference: CVE-2016-5617**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/184
NA	2016-10-25	4.4	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: MyISAM. **Reference: CVE-2016-5616**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/185
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.5.50 and earlier, 5.6.31 and earlier, and 5.7.13 and earlier allows remote	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-MYSQL-41116/186

			authenticated users to affect availability via vectors related to DML. **Reference: CVE-2016-5612**	oct2016-2881722.html	
NA	2016-10-25	4	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to DML. **Reference: CVE-2016-5609**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/187
Gain Information	2016-10-25	3.5	Unspecified vulnerability in Oracle MySQL 5.5.52 and earlier, 5.6.33 and earlier, and 5.7.15 and earlier allows remote administrators to affect confidentiality via vectors related to Server: Security: Encryption. **Reference: CVE-2016-5584**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/188
NA	2016-10-25	6.8	Unspecified vulnerability in Oracle MySQL 5.6.32 and earlier and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB. **Reference: CVE-2016-5507**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/189
NA	2016-10-25	6.8	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB. **Reference: CVE-2016-3495**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/190
NA	2016-10-25	6.8	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and	http://www.oracle.com/technetwork/sec	A-ORA-MYSQL-41116/191

			earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer. **Reference: CVE-2016-3492**	urity-advisory/cpuoct2016-2881722.html	
Mysql Connectors MySQL offers standard database driver connectivity for using MySQL with applications and tools that are compatible with industry standards ODBC and JDBC.					
NA	2016-10-25	6.8	Unspecified vulnerability in the MySQL Connector component 2.1.3 and earlier and 2.0.4 and earlier in Oracle MySQL allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Connector/Python. **Reference: CVE-2016-5598**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-MYSQL-41116/192
Netbeans NetBeans is a software development platform written in Java. The NetBeansPlatform allows applications to be developed from a set of modular software components called modules.					
NA	2016-10-25	4.6	Unspecified vulnerability in the NetBeans component in Oracle Fusion Middleware 8.1 allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5537**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-NETBE-41116/193
One-to-one Fulfillment Oracle One-to-One Fulfillment provides Oracle E-Business Suite applications with a centralized mechanism for managing fulfillment.					
NA	2016-10-25	5	Unspecified vulnerability in the Oracle One-to-One Fulfillment component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-	A-ORA-ONE-T-41116/194

			allows remote attackers to affect integrity via unknown vectors. **Reference: CVE-2016-5583**	2881722.html	
Outside In Technology Oracle Outside In Technology provides software developers with a comprehensive solution to access, transform, and control the contents of over 500 unstructured file formats.					
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, and CVE-2016-5579. **Reference: CVE-2016-5588**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/195
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, and CVE-2016-5588. **Reference: CVE-2016-5579**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/196

NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5579, and CVE-2016-5588. **Reference: CVE-2016-5578**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/197
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588. **Reference: CVE-2016-5577**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/198
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/199

			vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5577, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588. **Reference: CVE-2016-5574**		
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588. **Reference: CVE-2016-5558**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-OUTSI-41116/200
Peoplesoft Enterprise Human Capital Management Candidate Gateway Oracle's PeopleSoft Human Capital Management enables you to architect a global foundation for HR data and improved business processes. PeopleSoft Human Capital Management delivers a robust set of best-in-class human resources functionality that enables you to increase productivity, accelerate business performance, and lower your cost of ownership.					
NA	2016-10-25	4.9	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.2 allows remote administrators to affect confidentiality and integrity via vectors related to Candidate Gateway. **Reference: CVE-2016-8285**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/201

NA	2016-10-25	5.8	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to Talent Acquisition Manager. **Reference: CVE-2016-8292**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/202
Peoplesoft Enterprise Human Capital Management Time And Labor Oracle's PeopleSoft Time and Labor application is a flexible, integrated solution that gives organizations both intelligence and power through a single repository which helps them determine key performance indicators that are impacted by time-related data.					
Gain Information	2016-10-25	4	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.2 allows remote authenticated users to affect confidentiality via unknown vectors. **Reference: CVE-2016-8295**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/203
Peoplesoft Enterprise Peopletools PeopleTools is the foundation for all PeopleSoft Enterprise Applications, it is an essential software management tool for all PeopleSoft customers.					
NA	2016-10-25	4.9	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to LDAP. **Reference: CVE-2016-8296**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/204
Gain Information	2016-10-25	4	Unspecified vulnerability in the PeopleSoft	http://www.oracle.com/tec	A-ORA-PEOPL-41116/205

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote authenticated users to affect confidentiality via unknown vectors. **Reference: CVE-2016-8294**	hnetwork/security-advisory/cpuoct2016-2881722.html	
NA	2016-10-25	5.8	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote attackers to affect confidentiality and integrity via vectors related to Integration Broker, a different vulnerability than CVE-2016-5529 and CVE-2016-5530. **Reference: CVE-2016-8293**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/206
NA	2016-10-25	5.8	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote attackers to affect confidentiality and integrity via vectors related to Mobile Application Platform. **Reference: CVE-2016-8291**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/207
NA	2016-10-25	5.8	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote attackers to affect	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/208

			confidentiality and integrity via vectors related to Integration Broker, a different vulnerability than CVE-2016-5529 and CVE-2016-8293. **Reference: CVE-2016-5530**		
NA	2016-10-25	5.8	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote attackers to affect confidentiality and integrity via vectors related to Integration Broker, a different vulnerability than CVE-2016-5530 and CVE-2016-8293. **Reference: CVE-2016-5529**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/209
Peoplesoft Enterprise Supply Chain Management Services Procurement Oracle's PeopleSoft Supply Chain Management (SCM) provides a cohesive yet flexible solution for the synchronized supply chain, driving efficiencies in cost savings over your entire supply chain including your plan-to-produce and order-to-cash business processes.					
NA	2016-10-25	5.5	Unspecified vulnerability in the PeopleSoft Enterprise SCM Services Procurement component in Oracle PeopleSoft Products 9.1 and 9.2 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-5600**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PEOPL-41116/210
Platform Security For Java Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable,					

integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.					
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Platform Security for Java component in Oracle Fusion Middleware 12.1.3.0.0, 12.2.1.0.0, and 12.2.1.1.0 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-8281**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PLATF-41116/211
NA	2016-10-25	6.5	Unspecified vulnerability in the Oracle Platform Security for Java component in Oracle Fusion Middleware 12.1.3.0.0, 12.2.1.0.0, and 12.2.1.1.0 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5536**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PLATF-41116/212
Primavera P6 Enterprise Project Portfolio Management Primavera P6 Enterprise Project Portfolio Management is powerful tools for global project planning manage projects of any size with this cloud-based, robust, and easy-to-use solution for globally prioritizing, planning, managing, and executing projects, programs, and portfolios.					
NA	2016-10-25	5.5	Unspecified vulnerability in the Primavera P6 Enterprise Project Portfolio Management component in Oracle Primavera Products Suite 8.4, 15.x, and 16.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors. **Reference: CVE-2016-**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-PRIMA-41116/213

			5533		
Secure Global Desktop Oracle Secure Global Desktop (SGD) is a secure remote access solution for any cloud-hosted enterprise applications and desktops running on Microsoft Windows, Linux, Solaris and mainframe servers, from a wide range of popular client devices, including Windows PCs, Macs, Linux PCs, and tablets such as the Apple iPad and Android-based devices.					
NA	2016-10-25	5.5	Unspecified vulnerability in the Secure Global Desktop component in Oracle Virtualization 4.7 and 5.2 allows remote authenticated users to affect confidentiality and availability via vectors through Web Services. **Reference: CVE-2016-5580**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SECUR-41116/214
Shipping Execution NA					
NA	2016-10-25	5	Unspecified vulnerability in the Oracle Shipping Execution component in Oracle E-Business Suite 12.1.1 through 12.1.3 and 12.2.3 through 12.2.6 allows remote attackers to affect confidentiality via vectors related to Workflow Events. **Reference: CVE-2016-5532**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SHIPP-41116/215
Siebel Customer Order Management Oracle's Siebel Customer Order Management solutions simplify the complex and often frustrating process of tracking thousands of products across multiple catalogs and systems. They deliver deep customer insight that enables businesses to dynamically present targeted product bundles, offer intelligent cross-sell and up-sell opportunities, and achieve optimal prices for products and customer segments.					
NA	2016-10-25	5.5	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 16.1 allows remote authenticated users to affect confidentiality and integrity via vectors	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SIEBE-41116/216

			related to OpenUI. **Reference: CVE-2016-5560**		
NA	2016-10-25	4	Unspecified vulnerability in the Siebel Apps - Customer Order Management component in Oracle Siebel CRM 16.1 allows remote authenticated users to affect confidentiality via unknown vectors. **Reference: CVE-2016-5534**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SIEBE-41116/217
Solaris Cluster Oracle Solaris Cluster delivers unrivaled High Availability on the Oracle Solaris OS for the largest selection of enterprise applications and databases.					
NA	2016-10-25	2.1	Unspecified vulnerability in the Solaris Cluster component in Oracle Sun Systems Products Suite 3.3 and 4.3 allows local users to affect integrity via vectors related to Cluster check files. **Reference: CVE-2016-5525**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SOLAR-41116/218
Gain Information	2016-10-25	2.1	Unspecified vulnerability in the Solaris Cluster component in Oracle Sun Systems Products Suite 4.3 allows local users to affect confidentiality via vectors related to Cluster Geo. **Reference: CVE-2016-5508**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SOLAR-41116/219
Sun Zfs Storage Appliance Kit Oracle ZFS Storage Software Reduce Complexity, Risk, Inefficiency, and Cost Oracle ZFS Storage Appliances provide advanced software and Oracle exclusive co-engineering to protect data, speed tuning and troubleshooting and deliver high performance and high availability.					
NA	2016-10-25	4.6	Unspecified vulnerability in the Sun ZFS Storage Appliance Kit (AK) component in Oracle Sun	http://www.oracle.com/technetwork/security-	A-ORA-SUN Z-41116/220

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Systems Products Suite AK 2013 allows local users to affect confidentiality, integrity, and availability via vectors related to Core Services. **Reference: CVE-2016-5503**	advisory/cpuoct2016-2881722.html	
NA	2016-10-25	3.6	Unspecified vulnerability in the Sun ZFS Storage Appliance Kit (AK) component in Oracle Sun Systems Products Suite AK 2013 allows local users to affect confidentiality and integrity via vectors related to SMB Users. **Reference: CVE-2016-5492**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SUN Z-41116/221
NA	2016-10-25	4.9	Unspecified vulnerability in the Sun ZFS Storage Appliance Kit (AK) component in Oracle Sun Systems Products Suite AK 2013 allows local users to affect confidentiality via vectors related to Core Services. **Reference: CVE-2016-5486**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SUN Z-41116/222
Gain Information	2016-10-25	4.3	Unspecified vulnerability in the Sun ZFS Storage Appliance Kit (AK) component in Oracle Sun Systems Products Suite AK 2013 allows remote attackers to affect confidentiality via vectors related to Core Services. **Reference: CVE-2016-5481**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-SUN Z-41116/223
Vm Virtualbox Oracle VM VirtualBox is a free and open-source hypervisor for x86 computers from Oracle					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Corporation.					
NA	2016-10-25	2.1	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect availability via vectors related to Core, a different vulnerability than CVE-2016-5608. **Reference: CVE-2016-5613**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/224
Gain Information	2016-10-25	2.1	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality via vectors related to Core. **Reference: CVE-2016-5611**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/225
NA	2016-10-25	3.6	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality, integrity, and availability via vectors related to Core. **Reference: CVE-2016-5610**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/226
NA	2016-10-25	2.1	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect availability	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/227

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via vectors related to Core, a different vulnerability than CVE-2016-5613. **Reference: CVE-2016-5608**		
NA	2016-10-25	6.4	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.1.4 in Oracle Virtualization allows remote attackers to affect confidentiality and integrity via vectors related to VRDE. **Reference: CVE-2016-5605**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/228
NA	2016-10-25	7.2	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality, integrity, and availability via vectors related to Core, a different vulnerability than CVE-2016-5501. **Reference: CVE-2016-5538**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/229
NA	2016-10-25	7.2	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality, integrity, and availability via vectors related to Core, a different vulnerability than CVE-2016-5538. **Reference: CVE-2016-5501**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-VM VI-41116/230

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Webcenter Sites Oracle WebCenter is Oracle's portfolio of user engagement software products built on top of the JSF-based Oracle Application Development Framework. WebCenter Content competes in the Enterprise Content Management market. WebCenter Sites compete in the Web Experience Management market and WebCenter Portal competes in the self-service portal and content delivery market space.					
NA	2016-10-25	4.3	Unspecified vulnerability in the Oracle WebCenter Sites component in Oracle Fusion Middleware 12.2.1.0.0, 12.2.1.1.0, and 12.2.1.2.0 allows remote attackers to affect integrity via unknown vectors. **Reference: CVE-2016-5511**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBCE-41116/231
Weblogic Server WebLogic Server contains Java 2 Platform, Enterprise Edition (J2EE) technologies. J2EE is the standard platform for developing multitier enterprise applications based on the Java programming language.					
NA	2016-10-25	3.3	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 12.1.3.0, 12.2.1.0, and 12.2.1.1 allows local users to affect confidentiality and integrity via vectors related to CIE Related Components. **Reference: CVE-2016-5601**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBLO-41116/232
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, 12.2.1.0, and 12.2.1.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBLO-41116/233

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			5535		
NA	2016-10-25	7.5	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS-WebServices. **Reference: CVE-2016-5531**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBLO-41116/234
NA	2016-10-25	5	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0 and 12.1.3.0 allows remote attackers to affect availability via vectors related to Web Container. **Reference: CVE-2016-5488**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBLO-41116/235
NA	2016-10-25	10	Unspecified vulnerability in the Oracle Web Services component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, and 12.2.1.0.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAXWS Web Services Stack. **Reference: CVE-2016-3551**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	A-ORA-WEBLO-41116/236
NA	2016-10-25	9	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0,	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-WEBLO-41116/237

			12.1.3.0, and 12.2.1.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to JavaServer Faces. **Reference: CVE-2016-3505**	oct2016-2881722.html	
Pivotal Software					
Redis Redis is an open source (BSD licensed), in-memory data structure store, used as database, cache and message broker.					
Execute Code; Overflow	2016-10-28	7.5	A buffer overflow in Redis 3.2.x prior to 3.2.4 causes arbitrary code execution when a crafted command is sent. An out of bounds write vulnerability exists in the handling of the client-output-buffer-limit option during the CONFIG SET command for the Redis data structure store. A crafted CONFIG SET command can lead to an out of bounds write potentially resulting in code execution. **Reference: CVE-2016-8339**	NA	A-PIV-REDIS-41116/238
Realnetworks					
Realplayer RealPlayer is a user-friendly media player.					
NA	2016-10-28	4.3	Improper handling of a repeating VRAT chunk in qcpfformat.dll allows attackers to cause a Null pointer dereference and crash in RealNetworks RealPlayer 18.1.5.705 through a crafted .QCP media file.	https://www.exploit-db.com/exploits/40617/	A-REA-REALP-41116/239

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-9018		
Yandex					
Yandex Browser The quick and secure browser from Yandex for computers, as well as smartphones and tablets on Android and iOS (iPhone and iPad).					
Cross Site Scripting	2016-10-26	4.3	XSS in Yandex Browser Translator in Yandex browser for desktop for versions from 15.12 to 16.2 could be used by remote attacker for evaluation arbitrary javascript code. **Reference: CVE-2016-8506**	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/240
Cross Site Request Forgery	2016-10-26	4.3	CSRF of synchronization form in Yandex Browser for desktop before version 16.6 could be used by remote attacker to steal saved data in browser profile. **Reference: CVE-2016-8504**	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/241
NA	2016-10-26	5	Yandex Protect Anti-phishing warning in Yandex Browser for desktop from version 16.7 to 16.9 could be used by remote attacker for brute-forcing passwords from important web-resource with special JavaScript. **Reference: CVE-2016-8503**	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/242
NA	2016-10-26	5	Yandex Protect Anti-phishing warning in Yandex Browser for desktop from version 15.12.0 to 16.2 could be used by remote attacker for brute-forcing	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/243

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			passwords from important web-resource with special JavaScript. **Reference: CVE-2016-8502**		
Bypass	2016-10-26	5	Security WiFi bypass in Yandex Browser from version 15.10 to 15.12 allows remote attacker to sniff traffic in open or WEP-protected wi-fi networks despite of special security mechanism is enabled. **Reference: CVE-2016-8501**	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/244
Cross Site Scripting	2016-10-26	4.3	XSS in Yandex Browser BookReader in Yandex browser for desktop for versions before 16.6. could be used by remote attacker for evaluation arbitrary javascript code. **Reference: CVE-2016-8505**	https://browser.yandex.com/security/changelogs/	A-YAN-YANDE-41116/245
Application; Operating System (A/OS)					
Redhat/Shotwell Project					
Enterprise Linux/Shotwell Red Hat Enterprise Linux (RHEL) is a Linux distribution developed by Red Hat and targeted toward the commercial market/Shotwell is an image organizer designed to provide personal photo management for the GNOME.					
NA	2016-10-25	4.3	Shotwell version 0.22.0 (and possibly other versions) is vulnerable to a TLS/SSL certification validation flaw resulting in a potential for man in the middle attacks. **Reference: CVE-2016-1000033**	NA	A-RED-ENTER-41116/246
Hardware (H)					
Ruckus					
Wireless H500 The ZoneFlex H500 is a converged wired and wireless wall switch featuring Ruckus BeamFlex plus					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

smart antenna technology to deliver high-speed 802.					
Denial of Service	2016-10-25	5	Ruckus Wireless H500 web management interface denial of service **Reference: CVE-2016-1000215**	https://www.tripwire.com/state-of-security/vulnerability-management/ruckus-vulnerability/	H-RUC-WIREL-41116/247
Bypass	2016-10-25	5	Ruckus Wireless H500 web management interface authentication bypass **Reference: CVE-2016-1000214**	https://www.tripwire.com/state-of-security/vulnerability-management/ruckus-vulnerability/	H-RUC-WIREL-41116/248
Cross Site Request Forgery	2016-10-25	6.8	Ruckus Wireless H500 web management interface CSRF **Reference: CVE-2016-1000213**	https://www.tripwire.com/state-of-security/vulnerability-management/ruckus-vulnerability/	H-RUC-WIREL-41116/249
Operating System (OS)					
Brocade					
NetIron Os NetIron Operating System software is specialized in powering service provider networks over the last decade.					
Denial of Service; Overflow; Memory Corruption	2016-10-31	7.8	A memory corruption in the IPsec code path of Brocade NetIron OS on Brocade MLXs 5.8.00 through 5.8.00e, 5.9.00 through 5.9.00bd, 6.0.00, and 6.0.00a images could allow attackers to cause a denial of service (line card reset) via certain constructed IPsec control packets. **Reference: CVE-2016-8203**	http://www.brocade.com/en/backend-content/pdf-page.html?/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-168.pdf	O-BRO-NETIR-41116/250

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cisco					
Ios Xe IOS XE is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), introduced with the ASR 1000 series.					
NA	2016-10-27	4.3	A vulnerability in Cisco IOS XE Software running on Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause a configuration integrity change to the vty line configuration on an affected device. This vulnerability affects the following releases of Cisco IOS XE Software running on Cisco cBR-8 Converged Broadband Routers: All 3.16S releases, All 3.17S releases, Release 3.18.0S, Release 3.18.1S, Release 3.18.0SP. More Information: CSCuz62815. Known Affected Releases: 15.5(3)S2.9, 15.6(2)SP. Known Fixed Releases: 15.6(1.7)SP1, 16.4(0.183), 16.5(0.1). **Reference: CVE-2016-6438**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-cbr-8	O-CIS-IOS X-41116/251
Citrix					
Netscaler Application Delivery Controller Firmware NetScaler ADC, an advanced software-defined application delivery controller, is your networking power player.					
NA	2016-10-28	5.8	Unauthorized redirect vulnerability in Citrix NetScaler ADC before 10.1 135.8, 10.5 61.11, 11.0 65.31/65.35F and 11.1 47.14 allows a	https://support.citrix.com/article/CTX218361	O-CIT-NETSC-41116/252

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			remote attacker to steal session cookies of a legitimate AAA user via manipulation of Host header. **Reference: CVE-2016-9028**		
Google					
Android Android is an OS created by Google for use on mobile devices, such as smart phones and tablets.					
NA	2016-10-31	7.8	On Samsung Galaxy S4 through S7 devices, the "omacp" app ignores security information embedded in the OMACP messages resulting in remote unsolicited WAP Push SMS messages being accepted, parsed, and handled by the device, leading to unauthorized configuration changes, a subset of SVE-2016-6542. **Reference: CVE-2016-7991**	http://security.samsungmobile.com/smrupdate.html#SMR-AUG-2016	O-GOO-ANDRO-41116/253
Denial of Service; Execute Code; Overflow	2016-10-31	10	On Samsung Galaxy S4 through S7 devices, an integer overflow condition exists within libomacp.so when parsing OMACP messages (within WAP Push SMS messages) leading to a heap corruption that can result in Denial of Service and potentially remote code execution, a subset of SVE-2016-6542. **Reference: CVE-2016-7990**	http://security.samsungmobile.com/smrupdate.html#SMR-AUG-2016	O-GOO-ANDRO-41116/254

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

NA	2016-10-31	7.8	On Samsung Galaxy S4 through S7 devices, a malformed OTA WAP PUSH SMS containing an OMACP message sent remotely triggers an unhandled ArrayIndexOutOfBounds Exception in Samsung's implementation of the WifiServiceImpl class within wifi-service.jar. This causes the Android runtime to continually crash, rendering the device unusable until a factory reset is performed, a subset of SVE-2016-6542. **Reference: CVE-2016-7989**	http://security.samsungmobile.com/smrupdate.html#SMR-AUG-2016	O-GOO-ANDRO-41116/255
NA	2016-10-31	7.8	On Samsung Galaxy S4 through S7 devices, absence of permissions on the BroadcastReceiver responsible for handling the com.[Samsung].android.intent.action.SET_WIFI intent leads to unsolicited configuration messages being handled by wifi-service.jar within the Android Framework, a subset of SVE-2016-6542. **Reference: CVE-2016-7988**	http://security.samsungmobile.com/smrupdate.html#SMR-AUG-2016	O-GOO-ANDRO-41116/256
Linux					
Linux Kernel The Linux kernel is a Unix-like computer operating system kernel.					
Denial of Service	2016-10-16	7.8	The IP stack in the Linux kernel before 4.6	https://github.com/torvalds/l	O-LIN-LINUX-41116/257

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039. **Reference: CVE-2016-8666**	inux/commit/fac8e0f579695a3ecbc4d3cac369139d7f819971	
Denial of Service	2016-10-16	4.9	The XFS subsystem in the Linux kernel through 4.8.2 allows local users to cause a denial of service (fdatasync failure and system hang) by using the vfs syscall group in the trinity program, related to a "page lock order bug in the XFS seek hole/data implementation." **Reference: CVE-2016-8660**	https://bugzilla.redhat.com/show_bug.cgi?id=1384851	O-LIN-LINUX-41116/258
Denial of Service; Overflow	2016-10-16	5.6	Stack-based buffer overflow in the brcmf_cfg80211_start_ap function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.7.5 allows local users to cause a denial of service (system crash) or possibly have unspecified other	https://github.com/torvalds/linux/commit/ded89912156b1a47d940a0c954c43afbabd0c42c	O-LIN-LINUX-41116/259

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			impact via a long SSID Information Element in a command to a Netlink socket. **Reference: CVE-2016-8658**		
Denial of Service; Overflow; Gain Privileges	2016-10-16	7.2	The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code. **Reference: CVE-2016-7425**	https://bugzilla.redhat.com/show_bug.cgi?id=1377330	O-LIN-LINUX-41116/260
Gain Privileges	2016-10-16	3.6	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. **Reference: CVE-2016-7097**	https://github.com/torvalds/linux/commit/073931017b49d9458aa351605b43a7e34598caef	O-LIN-LINUX-41116/261
Denial of Service; Overflow; Memory Corruption	2016-10-16	4.9	The proc_keys_show function in security/keys/proc.c in the Linux kernel through 4.8.2, when the GNU Compiler Collection (gcc) stack	https://bugzilla.redhat.com/show_bug.cgi?id=1373966	O-LIN-LINUX-41116/262

			protector is enabled, uses an incorrect buffer size for certain timeout data, which allows local users to cause a denial of service (stack memory corruption and panic) by reading the /proc/keys file. **Reference: CVE-2016-7042**		
Denial of Service	2016-10-16	4.9	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option. **Reference: CVE-2016-6828**	https://github.com/torvalds/linux/commit/bb1fceca22492109be12640d49f5ea5a544c6bb4	O-LIN-LINUX-41116/263
Denial of Service	2016-10-16	4.9	drivers/infiniband/ulp/srpt/ib_srpt.c in the Linux kernel before 4.5.1 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an ABORT_TASK command to abort a device write operation. **Reference: CVE-2016-6327**	https://github.com/torvalds/linux/commit/51093254bf879bc9ce96590400a87897c7498463	O-LIN-LINUX-41116/264
Denial of Service	2016-10-16	4.9	fs/overlayfs/copy_up.c in the Linux kernel before 4.2.6 uses an incorrect cleanup code	https://github.com/torvalds/linux/commit/ab79efab0a0ba	O-LIN-LINUX-41116/265

			path, which allows local users to cause a denial of service (dentry reference leak) via filesystem operations on a large file in a lower overlayfs layer. **Reference: CVE-2015-8953**	01a74df782eb7fa44b044dae8b5	
Denial of Service	2016-10-16	2.1	The mbcache feature in the ext2 and ext4 filesystem implementations in the Linux kernel before 4.6 mishandles xattr block caching, which allows local users to cause a denial of service (soft lockup) via filesystem operations in environments that use many attributes, as demonstrated by Ceph and Samba. **Reference: CVE-2015-8952**	https://lwn.net/Articles/668718/	O-LIN-LINUX-41116/266
Denial of Service; Gain Privileges	2016-10-16	7.2	mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero. **Reference: CVE-2015-3288**	https://security-tracker.debian.org/tracker/CVE-2015-3288	O-LIN-LINUX-41116/267
Linux;Oracle					
Linux Kernel/Linux; Vm Server The Linux kernel is a Unix-like computer operating system kernel; A virtual machine server (VM server) hosts or runs virtual machines that run various operating systems and act as full computing platforms on their own through emulation and virtualization.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	2016-10-16	7.8	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666. **Reference: CVE-2016-7039**	https://patchwork.ozlabs.org/patch/680412/	O-LIN-LINUX-41116/268
Oracle					
Solaris Solaris is a Unix operating system originally developed by Sun Microsystems.					
NA	2016-10-25	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Lynx. **Reference: CVE-2016-5615**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/269
NA	2016-10-25	5.6	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect integrity and availability via vectors related to Kernel Zones. **Reference: CVE-2016-5606**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/270
NA	2016-10-25	4.9	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Kernel Zones.	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-	O-ORA-SOLAR-41116/271

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-5576	2881722.html	
NA	2016-10-25	5	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows remote attackers to affect confidentiality via unknown vectors. **Reference: CVE-2016-5566**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/272
NA	2016-10-25	2.6	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows remote attackers to affect availability via vectors related to IKE. **Reference: CVE-2016-5561**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/273
NA	2016-10-25	4	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect integrity via vectors related to Kernel. **Reference: CVE-2016-5559**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/274
NA	2016-10-25	4.7	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect availability via unknown vectors. **Reference: CVE-2016-5553**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/275
NA	2016-10-25	7.2	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect confidentiality, integrity, and availability via vectors related to Kernel/X86. **Reference: CVE-2016-5544**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/276

NA	2016-10-25	4.6	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5487**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/277
NA	2016-10-25	1.9	Unspecified vulnerability in Oracle Sun Solaris 10 allows local users to affect integrity via vectors related to Bash. **Reference: CVE-2016-5480**	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html	O-ORA-SOLAR-41116/278

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10