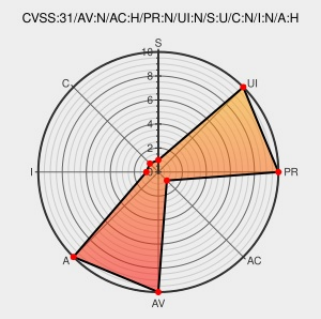
CVE-2021-45105

Published on: Not Yet Published

Last Modified on: 10/06/2022 05:31:00 PM UTC

CVE-2021-45105

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Log4j from Apache contain the following vulnerability:

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

CVE-2021-45105 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

Vulnerability Patch/Work Around

Implement one of the following mitigation techniques: * Java 8 (or later) users should upgrade to release 2.17.0. Alternatively, this can be mitigated in configuration: * In PatternLayout in the logging configuration, replace Context Lookups like `${ctx:loginId}` or `$${ctx:loginId}` with Thread Context Map patterns (%X, %mdc, or %MDC). * Otherwise, in the configuration, remove references to Context Lookups like `${ctx:loginId}` or `$${ctx:loginId}` where they originate from sources external to the application such as HTTP headers or user input.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 2852-1] apache-log4j2 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20211226 [SECURITY] [DLA 2852-1] apache-log4j2 security update
Security Advisory	psirt.global.sonicwall.com text/html	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032
Debian -- Security Information -- DSA-5024-1 apache-log4j2	www.debian.org Depreciated Link text/html	DEBIAN DSA-5024
Oracle Critical Patch Update Advisory - April 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2022.html
[SECURITY] Fedora 35 Update: log4j-2.17.0-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-abbe24e41c
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-501673.pdf
CVE-2021-45105 Apache Log4j Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211218-0001/
Oracle Critical Patch Update Advisory - January 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2022.html
ZDI-21-1541 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-1541/
Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021	tools.cisco.com text/html	CISCO 20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
oss-security - CVE-2021-45105: Apache Log4j2 does not always protect from infinite recursion in lookup evaluation	www.openwall.com text/html	MLIST [oss-security] 20211218 CVE-2021-45105: Apache Log4j2 does not always protect from infinite recursion in lookup evaluation
Log4j – Apache Log4j Security Vulnerabilities	logging.apache.org text/html	MISC logging.apache.org/log4j/2.x/security.html
[SECURITY] Fedora 34 Update: log4j-2.17.0-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-5c9d12a93e
VU#930724 - Apache Log4j allows insecure JNDI lookups	www.kb.cert.org text/html	CERT-VN VU#930724
Oracle Critical Patch Update Advisory - July 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujul2022.html

Related QID Numbers

178945 Debian Security Update for apache-log4j2 (DSA 5024-1)

178956 Debian Security Update for apache-log4j2 (DLA 2852-1)

198613 Ubuntu Security Notification for Apache Log4j 2 Vulnerability (USN-5203-1)

198626 Ubuntu Security Notification for Apache Log4j 2 Vulnerabilities (USN-5222-1)

20240 Oracle Database 19c Critical Patch Update - January 2022

20241 Oracle Database 12.2.0.1 Critical Patch Update - January 2022

20242 Oracle Database 12.2.0.1 Critical Patch Update - January 2022 (Unauthenticated)

20252 IBM DB2 Security Update for Log4j (6528672,6549888)

20289 Oracle Database 19c Critical OJVM Patch Update - January 2022

240209 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1296)

240210 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1297)

282198 Fedora Security Update for log4j (FEDORA-2021-5c9d12a93e) (Log4Shell)

282200 Fedora Security Update for log4j (FEDORA-2021-abbe24e41c) (Log4Shell)

317120 Cisco Unified Communications Manager (CUCM) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

317121 Cisco Unified Communications Manager IM and Presence Service (formerly CUPS) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

317123 Cisco UCS Central Software Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

353090 Amazon Linux Security Advisory for aws-kinesis-agent : ALAS2-2021-1733

376192 Elasticsearch Logstash Log4j Remote Code Execution (RCE) Vulnerability

376194 Apache Log4j Denial of Service (DOS) Vulnerability (Log4Shell)

376195 Apache Log4j Denial of Service (DOS) Vulnerability (Log4Shell) Detected Based on Qualys Log4j scan Utility

376230 Dell EMC NetWorker Apache Log4j multiple Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

376231 Dell EMC NetWorker Server Apache Log4j multiple Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

376425 Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (Log4Shell) (Doc_ID_2817011.1)

376477 Autonomous Health Framework (AHF) Multiple Vulnerabilities (Log4Shell) (Doc ID 2828415.1)

690756 Free Berkeley Software Distribution (FreeBSD) Security Update for opensearch (d1be3d73-6737-11ec-9eea-589cfc007716)

730318 Palo Alto Networks (PAN-OS) Log4j Multiple Vulnerabilities (PAN-184592) (Log4Shell)

730329 Dell EMC NetWorker Virtual Edition Multiple Apache Log4j Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

730331 Dell EMC NetWorker Virtual Edition multiple Apache Log4j Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

730362 Neo4j Database Server Affected by Apache Log4j Security Vulnerability

730367 Dell EMC SRM Remote Code Execution (RCE) Vulnerability (DSA-2021-301)

730371 McAfee Web Gateway Multiple Vulnerabilities (WP-3335,WP-4131,WP-4159,WP-4237,WP-4259,WP-4329,WP-4348,WP-4355,WP-4376,WP-4407,WP-4421)

751534 OpenSUSE Security Update for log4j (openSUSE-SU-2021:4118-1)

751546 OpenSUSE Security Update for log4j (openSUSE-SU-2021:1605-1)

87473 Cisco Nexus Dashboard Fabric Controller (Formerly DCNM) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

87482 Oracle WebLogic Server Multiple Vulnerabilities (Log4Shell) (Doc_ID_2828556.1)

87483 Oracle WebLogic Server Multiple Vulnerabilities (Log4Shell) (Doc_ID_2817011.1)

Exploit/POC from Github

Log4j_dos_CVE-2021-45105

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Log4j	All	All	All	All
Application	Apache	Log4j	2.0	-	All	All
Application	Apache	Log4j	2.0	alpha1	All	All
Application	Apache	Log4j	2.0	alpha2	All	All
Application	Apache	Log4j	2.0	beta1	All	All
Application	Apache	Log4j	2.0	beta2	All	All
Application	Apache	Log4j	2.0	beta3	All	All
Application	Apache	Log4j	2.0	beta3-rc1	All	All
Application	Apache	Log4j	2.0	beta3-rc2	All	All
Application	Apache	Log4j	2.0	beta4	All	All
Application	Apache	Log4j	2.0	beta4-rc1	All	All
Application	Apache	Log4j	2.0	beta5	All	All
Application	Apache	Log4j	2.0	beta6	All	All
Application	Apache	Log4j	2.0	beta6-rc1	All	All
Application	Apache	Log4j	2.0	beta7	All	All
Application	Apache	Log4j	2.0	beta7-rc1	All	All
Application	Apache	Log4j	2.0	beta7-rc2	All	All
Application	Apache	Log4j	2.0	beta8	All	All
Application	Apache	Log4j	2.0	beta8-rc1	All	All
Application	Apache	Log4j	2.0	beta9	All	All
Application	Apache	Log4j	2.0	rc1	All	All
Application	Apache	Log4j	2.0	rc1-rc1	All	All

Application	Apache	Log4j	2.0	rc2	All	All
Application	Apache	Log4j	2.0.1	All	All	All
Application	Apache	Log4j	2.0.2	All	All	All
Application	Apache	Log4j	2.1	-	All	All
Application	Apache	Log4j	2.1	rc2	All	All
Application	Apache	Log4j	2.1	rc3	All	All
Application	Apache	Log4j	2.10.0	-	All	All
Application	Apache	Log4j	2.10.0	rc1	All	All
Application	Apache	Log4j	2.11.0	-	All	All
Application	Apache	Log4j	2.11.0	rc1	All	All
Application	Apache	Log4j	2.11.1	-	All	All
Application	Apache	Log4j	2.11.1	rc1	All	All
Application	Apache	Log4j	2.11.2	-	All	All
Application	Apache	Log4j	2.11.2	rc1	All	All
Application	Apache	Log4j	2.11.2	rc2	All	All
Application	Apache	Log4j	2.11.2	rc3	All	All
Application	Apache	Log4j	2.12.0	-	All	All
Application	Apache	Log4j	2.12.0	rc1	All	All
Application	Apache	Log4j	2.12.0	rc2	All	All
Application	Apache	Log4j	2.12.1	-	All	All
Application	Apache	Log4j	2.12.1	rc1	All	All
Application	Apache	Log4j	2.12.2	-	All	All
Application	Apache	Log4j	2.12.2	rc1	All	All
Application	Apache	Log4j	2.13.0	-	All	All
Application	Apache	Log4j	2.13.0	rc1	All	All
Application	Apache	Log4j	2.13.0	rc2	All	All
Application	Apache	Log4j	2.13.1	-	All	All
Application	Apache	Log4j	2.13.1	rc1	All	All
Application	Apache	Log4j	2.13.1	rc2	All	All
Application	Apache	Log4j	2.13.2	-	All	All
Application	Apache	Log4j	2.13.2	rc1	All	All
Application	Apache	Log4j	2.13.3	-	All	All
Application	Apache	Log4j	2.13.3	rc1	All	All
Application	Apache	Log4j	2.14.0	-	All	All
Application	Apache	Log4j	2.14.0	rc1	All	All
Application	Apache	Log4j	2.14.1	-	All	All

Application	Apache	Log4j	2.14.1	rc1	All	All
Application	Apache	Log4j	2.15.0	-	All	All
Application	Apache	Log4j	2.15.0	rc1	All	All
Application	Apache	Log4j	2.15.0	rc2	All	All
Application	Apache	Log4j	2.15.1	rc1	All	All
Application	Apache	Log4j	2.16.0	-	All	All
Application	Apache	Log4j	2.16.0	rc1	All	All
Application	Apache	Log4j	2.2	All	All	All
Application	Apache	Log4j	2.3	All	All	All
Application	Apache	Log4j	2.4	All	All	All
Application	Apache	Log4j	2.4.1	All	All	All
Application	Apache	Log4j	2.5	-	All	All
Application	Apache	Log4j	2.5	rc1	All	All
Application	Apache	Log4j	2.6	-	All	All
Application	Apache	Log4j	2.6	rc1	All	All
Application	Apache	Log4j	2.6.1	-	All	All
Application	Apache	Log4j	2.6.1	rc1	All	All
Application	Apache	Log4j	2.6.2	-	All	All
Application	Apache	Log4j	2.6.2	rc1	All	All
Application	Apache	Log4j	2.7	-	All	All
Application	Apache	Log4j	2.7	rc1	All	All
Application	Apache	Log4j	2.7	rc2	All	All
Application	Apache	Log4j	2.8	-	All	All
Application	Apache	Log4j	2.8	rc1	All	All
Application	Apache	Log4j	2.8.1	-	All	All
Application	Apache	Log4j	2.8.1	rc1	All	All
Application	Apache	Log4j	2.8.2	-	All	All
Application	Apache	Log4j	2.8.2	rc1	All	All
Application	Apache	Log4j	2.9.0	-	All	All
Application	Apache	Log4j	2.9.0	rc1	All	All
Application	Apache	Log4j	2.9.1	rc1	All	All
Application	Apache	Log4j	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All

Application	Netapp	Cloud Manager	-	All	All	All
Application	Oracle	Agile Engineering Data Management	6.2.1.0	All	All	All
Application	Oracle	Agile Plm	9.3.6	All	All	All
Application	Oracle	Agile Plm Mcad Connector	3.6	All	All	All
Application	Oracle	Autovue For Agile Product Lifecycle Management	21.0.2	All	All	All
Application	Oracle	Banking Deposits And Lines Of Credit Servicing	2.12.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.12.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.7.1	All	All	All
Application	Oracle	Banking Loans Servicing	2.12.0	All	All	All
Application	Oracle	Banking Party Management	2.7.0	All	All	All
Application	Oracle	Banking Payments	14.5	All	All	All
Application	Oracle	Banking Platform	2.12.0	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Banking Platform	2.7.1	All	All	All
Application	Oracle	Banking Trade Finance	14.5	All	All	All
Application	Oracle	Banking Treasury Management	14.5	All	All	All
Application	Oracle	Business Intelligence	5.5.0.0.0	All	All	All
Application	Oracle	Communications Asap	7.3	All	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0.0.4	All	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0.0.5	All	All	All
Application	Oracle	Communications Cloud Native Core Console	1.9.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	1.15.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	1.15.1	All	All	All
Application	Oracle	Communications Cloud Native Core Network Slice Selection Function	1.8.0	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.15.0	All	All	All
Application	Oracle	Communications Cloud Native Core Security Edge Protection Proxy	1.7.0	All	All	All
Application	Oracle	Communications Cloud Native Core Service Communication Proxy	1.15.0	All	All	All
Application	Oracle	Communications Cloud Native Core Unified Data Repository	1.15.0	All	All	All
Application	Oracle	Communications Convergence	3.0.2.2.0	All	All	All
Application	Oracle	Communications Convergence	3.0.3.0	All	All	All
Application	Oracle	Communications Convergent Charging Controller	6.0.1.0.0	All	All	All

Application	Oracle	Communications Convergent Charging Controller	All	All	All	All
Application	Oracle	Communications Diameter Signaling Router	All	All	All	All
Application	Oracle	Communications Eagle Element Management System	46.6	All	All	All
Application	Oracle	Communications Eagle Ftp Table Base Retrieval	4.5	All	All	All
Application	Oracle	Communications Element Manager	All	All	All	All
Application	Oracle	Communications Evolved Communications Application Server	7.1	All	All	All
Application	Oracle	Communications Interactive Session Recorder	6.3	All	All	All
Application	Oracle	Communications Interactive Session Recorder	6.4	All	All	All
Application	Oracle	Communications Ip Service Activator	7.4.0	All	All	All
Application	Oracle	Communications Messaging Server	8.1	All	All	All
Application	Oracle	Communications Network Charging And Control	6.0.1.0.0	All	All	All
Application	Oracle	Communications Network Charging And Control	All	All	All	All
Application	Oracle	Communications Network Integrity	7.3.6	All	All	All
Application	Oracle	Communications Performance Intelligence Center	10.4.0.3	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.4	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.5	All	All	All
Application	Oracle	Communications Services Gatekeeper	7.0	All	All	All
Application	Oracle	Communications Service Broker	6.2	All	All	All
Application	Oracle	Communications Session Report Manager	All	All	All	All
Application	Oracle	Communications Session Route Manager	All	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.3.5	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.1	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.2	All	All	All
Application	Oracle	Communications User Data Repository	12.4	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2.0.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2.1	All	All	All
Application	Oracle	Data Integrator	12.2.1.3.0	All	All	All
Application	Oracle	Data Integrator	12.2.1.4.0	All	All	All
Application	Oracle	E-business Suite	12.2	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.4.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.5.0.0	All	All	All
Application	Oracle	Enterprise Manager For Peoplesoft	13.4.1.1	All	All	All
Application	Oracle	Enterprise Manager For Peoplesoft	13.5.1.1	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	All	All	All	All

Application	Oracle	Financial Services Model Management And Governance	8.0.8.0.0	All	All	All
Application	Oracle	Financial Services Model Management And Governance	8.1.0.0.0	All	All	All
Application	Oracle	Financial Services Model Management And Governance	8.1.1.0.0	All	All	All
Application	Oracle	Flexcube Universal Banking	11.83.3	All	All	All
Application	Oracle	Flexcube Universal Banking	14.5	All	All	All
Application	Oracle	Flexcube Universal Banking	All	All	All	All
Application	Oracle	Flexcube Universal Banking	All	All	All	All
Application	Oracle	Healthcare Data Repository	8.1.1	All	All	All
Application	Oracle	Healthcare Foundation	All	All	All	All
Application	Oracle	Healthcare Master Person Index	5.0.1	All	All	All
Application	Oracle	Healthcare Translational Research	4.1.0	All	All	All
Application	Oracle	Healthcare Translational Research	4.1.1	All	All	All
Application	Oracle	Health Sciences Empirica Signal	9.1.0.6	All	All	All
Application	Oracle	Health Sciences Empirica Signal	9.2.0.0	All	All	All
Application	Oracle	Health Sciences Inform	6.2.1.1	All	All	All
Application	Oracle	Health Sciences Inform	6.3.2.1	All	All	All
Application	Oracle	Health Sciences Inform	7.0.0.0	All	All	All
Application	Oracle	Health Sciences Information Manager	All	All	All	All
Application	Oracle	Hospitality Suite8	8.13.0	All	All	All
Application	Oracle	Hospitality Suite8	8.14.0	All	All	All
Application	Oracle	Hospitality Token Proxy Service	19.2	All	All	All
Application	Oracle	Hyperion Bi	All	All	All	All
Application	Oracle	Hyperion Data Relationship Management	All	All	All	All
Application	Oracle	Hyperion Infrastructure Technology	All	All	All	All
Application	Oracle	Hyperion Planning	All	All	All	All
Application	Oracle	Hyperion Profitability And Cost Management	All	All	All	All
Application	Oracle	Hyperion Tax Provision	All	All	All	All
Application	Oracle	Identity Management Suite	12.2.1.3.0	All	All	All
Application	Oracle	Identity Management Suite	12.2.1.4.0	All	All	All
Application	Oracle	Identity Manager Connector	9.1.0	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Insurance Data Gateway	1.0.1	All	All	All
Application	Oracle	Insurance Insbridge Rating And Underwriting	5.2.0	All	All	All
Application	Oracle	Insurance Insbridge Rating And Underwriting	5.6.1.0	All	All	All

Application	Oracle	Insurance Insbridge Rating And Underwriting	All	All	All	All
Application	Oracle	Jdeveloper	12.2.1.4.0	All	All	All
Application	Oracle	Managed File Transfer	12.2.1.3.0	All	All	All
Application	Oracle	Managed File Transfer	12.2.1.4.0	All	All	All
Application	Oracle	Management Cloud Engine	1.5.0	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Payment Interface	19.1	All	All	All
Application	Oracle	Payment Interface	20.3	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.59	All	All	All
Application	Oracle	Primavera Gateway	21.12.0	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	21.12.0.0	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	All	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	All	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	19.12	All	All	All
Application	Oracle	Primavera Unifier	20.12	All	All	All
Application	Oracle	Primavera Unifier	21.12	All	All	All
Application	Oracle	Retail Back Office	14.1	All	All	All
Application	Oracle	Retail Central Office	14.1	All	All	All
Application	Oracle	Retail Customer Insights	15.0.2	All	All	All
Application	Oracle	Retail Customer Insights	16.0.2	All	All	All
Application	Oracle	Retail Data Extractor For Merchandising	15.0.2	All	All	All
Application	Oracle	Retail Data Extractor For Merchandising	16.0.2	All	All	All
Application	Oracle	Retail Eftlink	16.0.3	All	All	All
Application	Oracle	Retail Eftlink	17.0.2	All	All	All
Application	Oracle	Retail Eftlink	18.0.1	All	All	All
Application	Oracle	Retail Eftlink	19.0.1	All	All	All
Application	Oracle	Retail Eftlink	20.0.1	All	All	All
Application	Oracle	Retail Eftlink	21.0.0	All	All	All
Application	Oracle	Retail Financial Integration	14.1.3.2	All	All	All

Application	Oracle	Retail Financial Integration	15.0.3.1	All	All	All
Application	Oracle	Retail Financial Integration	19.0.0	All	All	All
Application	Oracle	Retail Financial Integration	19.0.1	All	All	All
Application	Oracle	Retail Financial Integration	All	All	All	All
Application	Oracle	Retail Integration Bus	14.1.3	All	All	All
Application	Oracle	Retail Integration Bus	14.1.3.2	All	All	All
Application	Oracle	Retail Integration Bus	15.0.3.1	All	All	All
Application	Oracle	Retail Integration Bus	19.0.0	All	All	All
Application	Oracle	Retail Integration Bus	19.0.1	All	All	All
Application	Oracle	Retail Integration Bus	All	All	All	All
Application	Oracle	Retail Integration Bus	All	All	All	All
Application	Oracle	Retail Invoice Matching	15.0.3	All	All	All
Application	Oracle	Retail Invoice Matching	16.0.3	All	All	All
Application	Oracle	Retail Merchandising System	16.0.3	All	All	All
Application	Oracle	Retail Merchandising System	19.0.1	All	All	All
Application	Oracle	Retail Order Broker	16.0	All	All	All
Application	Oracle	Retail Order Broker	18.0	All	All	All
Application	Oracle	Retail Order Broker	19.1	All	All	All
Application	Oracle	Retail Order Management System	19.5	All	All	All
Application	Oracle	Retail Point-of-service	14.1	All	All	All
Application	Oracle	Retail Predictive Application Server	14.1.3.46	All	All	All
Application	Oracle	Retail Predictive Application Server	15.0.3.115	All	All	All
Application	Oracle	Retail Predictive Application Server	16.0.3.240	All	All	All
Application	Oracle	Retail Price Management	13.2	All	All	All
Application	Oracle	Retail Price Management	14.0.4	All	All	All
Application	Oracle	Retail Price Management	14.1.3.0	All	All	All
Application	Oracle	Retail Price Management	15.0.3.0	All	All	All
Application	Oracle	Retail Price Management	16.0.3.0	All	All	All
Application	Oracle	Retail Returns Management	14.1	All	All	All
Application	Oracle	Retail Service Backbone	14.1.3	All	All	All
Application	Oracle	Retail Service Backbone	14.1.3.2	All	All	All
Application	Oracle	Retail Service Backbone	15.0.3.1	All	All	All
Application	Oracle	Retail Service Backbone	19.0.0	All	All	All
Application	Oracle	Retail Service Backbone	19.0.1	All	All	All
Application	Oracle	Retail Service Backbone	19.0.1.0	All	All	All

Application	Oracle	Retail Service Backbone	All	All	All	All
Application	Oracle	Retail Store Inventory Management	14.0.4.13	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1.3.14	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1.3.5	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0.3.3	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0.3.8	All	All	All
Application	Oracle	Retail Store Inventory Management	16.0.3.7	All	All	All
Application	Oracle	Siebel Ui Framework	All	All	All	All
Application	Oracle	Sql Developer	All	All	All	All
Application	Oracle	Taleo Platform	All	All	All	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.3.0	All	All	All
Application	Oracle	Utilities Framework	All	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.4.0	All	All	All
Application	Oracle	Webcenter Sites	12.2.1.3.0	All	All	All
Application	Oracle	Webcenter Sites	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
Hardware	Sonicwall	6bk1602-0aa12-0tp0	-	All	All	All
Operating System	Sonicwall	6bk1602-0aa12-0tp0 Firmware	All	All	All	All
Hardware	Sonicwall	6bk1602-0aa22-0tp0	-	All	All	All
Operating System	Sonicwall	6bk1602-0aa22-0tp0 Firmware	All	All	All	All
Hardware	Sonicwall	6bk1602-0aa32-0tp0	-	All	All	All
Operating System	Sonicwall	6bk1602-0aa32-0tp0 Firmware	All	All	All	All
Hardware	Sonicwall	6bk1602-0aa42-0tp0	-	All	All	All
Operating System	Sonicwall	6bk1602-0aa42-0tp0 Firmware	All	All	All	All
Hardware	Sonicwall	6bk1602-0aa52-0tp0	-	All	All	All

Operating System	Sonicwall	6bk1602-0aa52-0tp0 Firmware	All	All	All	All
Application	Sonicwall	Email Security	All	All	All	All
Application	Sonicwall	Network Security Manager	All	All	All	All
Application	Sonicwall	Network Security Manager	All	All	All	All
Application	Sonicwall	Web Application Firewall	All	All	All	All

cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta3-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta3-rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta4-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta5:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta6:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta6-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta7:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta7-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta7-rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta8:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta8-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta9:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:rc1-rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.1:rc3:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.10.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.10.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.2:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.2:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.11.2:rc3:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.2:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.12.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.2:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.3:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.13.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.14.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.14.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.14.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.14.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.15.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.15.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.15.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.15.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.16.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.16.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.3:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.5:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.5:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6.2:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.6.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.7:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.7:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8:rc1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8.1:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8.2:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.8.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.9.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.9.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.9.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:

cpe:2.3:a:netapp:cloud_manager:-:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:agile_engineering_data_management:6.2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:agile_plm:9.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:agile_plm_mcad_connector:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:autovue_for_agile_product_lifecycle_management:21.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_deposits_and_lines_of_credit_servicing:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_enterprise_default_management:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_enterprise_default_management:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_loans_servicing:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_party_management:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_payments:14.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_platform:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_platform:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_platform:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_trade_finance:14.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:banking_treasury_management:14.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:business_intelligence:5.5.0.0.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:communications_asap:7.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_billing_and_revenue_management:12.0.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_billing_and_revenue_management:12.0.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_console:1.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_function_cloud_native_environment:1.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_repository_function:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_repository_function:1.15.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_slice_selection_function:1.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_policy:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_security_edge_protection_proxy:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_service_communication_proxy:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_unified_data_repository:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_convergence:3.0.2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_convergence:3.0.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_convergent_charging_controller:6.0.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_convergent_charging_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_diameter_signaling_router:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_eagle_element_management_system:46.6:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_eagle_ftp_table_base_retrieval:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_element_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_evolved_communications_application_server:7.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_interactive_session_recorder:6.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_interactive_session_recorder:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_ip_service_activator:7.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_messaging_server:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_network_charging_and_control:6.0.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_network_charging_and_control:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_network_integrity:7.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_performance_intelligence_center:10.4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_pricing_design_center:12.0.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_pricing_design_center:12.0.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_services_gatekeeper:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_service_broker:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_session_report_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_session_route_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_unified_inventory_management:7.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_unified_inventory_management:7.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_unified_inventory_management:7.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_user_data_repository:12.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_webrtc_session_controller:7.2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_webrtc_session_controller:7.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:data_integrator:12.2.1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:data_integrator:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:e-business_suite:12.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:enterprise_manager_base_platform:13.4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:enterprise_manager_base_platform:13.5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:enterprise_manager_for_peoplesoft:13.4.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:enterprise_manager_for_peoplesoft:13.5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:enterprise_manager_ops_center:12.4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:financial_services_model_management_and_governance:8.0.8.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:financial_services_model_management_and_governance:8.1.0.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:financial_services_model_management_and_governance:8.1.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:flexcube_universal_banking:11.83.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:flexcube_universal_banking:14.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:flexcube_universal_banking:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:flexcube_universal_banking:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:healthcare_data_repository:8.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:healthcare_foundation:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:healthcare_master_person_index:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:healthcare_translational_research:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:healthcare_translational_research:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_empirica_signal:9.1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_empirica_signal:9.2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_inform:6.2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_inform:6.3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_inform:7.0.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_information_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hospitality_suite8:8.13.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hospitality_suite8:8.14.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hospitality_token_proxy_service:19.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_bi\+:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_data_relationship_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_infrastructure_technology:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_planning:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_profitability_and_cost_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:hyperion_tax_provision:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:identity_management_suite:12.2.1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:identity_management_suite:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:identity_manager_connector:9.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:instantis_enterprisetrack:17.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:instantis_enterprisetrack:17.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:instantis_enterprisetrack:17.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:insurance_data_gateway:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:5.6.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:jdeveloper:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:managed_file_transfer:12.2.1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:managed_file_transfer:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:management_cloud_engine:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql_enterprise_monitor:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:payment_interface:19.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:payment_interface:20.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.58:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.59:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_gateway:21.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_p6_enterprise_project_portfolio_management:21.12.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_p6_enterprise_project_portfolio_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_p6_enterprise_project_portfolio_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_unifier:18.8:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_unifier:19.12:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_unifier:20.12:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:primavera_unifier:21.12:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_back_office:14.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_central_office:14.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_customer_insights:15.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_customer_insights:16.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_data_extractor_for_merchandising:15.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_data_extractor_for_merchandising:16.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:16.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:17.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:18.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:19.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:20.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_eftlink:21.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_financial_integration:14.1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_financial_integration:15.0.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_financial_integration:19.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_financial_integration:19.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_financial_integration:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:14.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:14.1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:15.0.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:19.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:19.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_integration_bus:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_invoice_matching:15.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_invoice_matching:16.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_merchandising_system:16.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_merchandising_system:19.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_order_broker:16.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_order_broker:18.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_order_broker:19.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_order_management_system:19.5:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_point-of-service:14.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_predictive_application_server:14.1.3.46:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_predictive_application_server:15.0.3.115:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_predictive_application_server:15.0.3.113:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_predictive_application_server:16.0.3.240:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_price_management:13.2:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_price_management:14.0.4:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_price_management:14.1.3.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_price_management:15.0.3.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_price_management:16.0.3.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_returns_management:14.1:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:14.1.3:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:14.1.3.2:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:15.0.3.1:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:19.0.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:19.0.1:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:19.0.1.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_service_backbone:*:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:14.0.4.13:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:14.1.3.14:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:14.1.3.5:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:15.0.3.3:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:15.0.3.8:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_store_inventory_management:16.0.3.7:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:siebel_ui_framework:*:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:sql_developer:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:taleo_platform:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:utilities_framework:4.4.0.0.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:utilities_framework:4.4.0.2.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:utilities_framework:4.4.0.3.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:utilities_framework:*:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_portal:12.2.1.3.0:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_portal:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_sites:12.2.1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_sites:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:6bk1602-0aa12-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:6bk1602-0aa12-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:6bk1602-0aa22-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:6bk1602-0aa22-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:6bk1602-0aa32-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:6bk1602-0aa32-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:6bk1602-0aa42-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:6bk1602-0aa42-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:6bk1602-0aa52-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:6bk1602-0aa52-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:a:sonicwall:email_security:*:*:*:*:*:*:*:*:

cpe:2.3:a:sonicwall:network_security_manager:*:*:*:*:on-premises:*:*:*:

cpe:2.3:a:sonicwall:network_security_manager:*:*:*:*:saas:*:*:*:

cpe:2.3:a:sonicwall:web_application_firewall:*:*:*:*:*:*:*:*:

Discovery Credit

Independently discovered by Hideki Okamoto of Akamai Technologies, Guy Lederfein of Trend Micro Research working with Trend Micro’s Zero Day Initiative, and another anonymous vulnerability researcher

Social Mentions

Source	Title	Posted (UTC)
@seolsson	@eltronnnnn @vxunderground @cstromblad It's referenced as DOS by log4j now (CVE-2021-45105). Fixed in 2.17. Can'… twitter.com/i/web/status/1…	2021-12-18 06:32:17
@ohhara_shiojiri	CVE-2021-45105になるのかな。	2021-12-18 06:53:56

@CGuntur	CVE-2021-45105 => addressed in log4j-core 2.17.0 CVSS: 7.5 Currently labeled as a Denial of Service vulnerability.	2021-12-18 06:58:47
@fguime	Thats it! I'm not logging anything anymore! (CVE-2021-45105). Just go nna close my eyes… and go to my happy place https://t.co/ust2jgGCQt	2021-12-18 07:12:32
@_r_netsec	log4j 2.17.0 Released to Fix CVSS 7.5 Denial of Service (CVE-2021-45105) logging.apache.org/log4j/2.x/secu…	2021-12-18 07:13:07
@beingsheerazali	log4j 2.17.0 Released to Fix CVSS 7.5 Denial of Service (CVE-2021-45105) logging.apache.org/log4j/2.x/secu… #infosec #pentest #bugbounty RT @_r_netsec	2021-12-18 07:14:19
@rushyo	The new CVE-2021-45105 log4j DoS vuln has been a matter of public record for a few days now but no vendor has come… twitter.com/i/web/status/1…	2021-12-18 07:16:22
@kasa_zip	あれ... Log4j 2.17.0が出てる...CVE-2021-45105が新しく出てきてた. あとCVE-2021-45046のCVSSも9.0に変更されてるし、色々と追加で明らかになった感じなんかな? logging.apache.org/log4j/2.x/secu…	2021-12-18 07:20:27
@seolsson	I belive CVE-2021-45105 fixed in log4j 2.17 affects few systems (or at least few that are already on 2.15+). Other… twitter.com/i/web/status/1…	2021-12-18 07:20:44
@akira0422	仕事増やさんといて〜	2021-12-18 07:20:59
@ghetto_9912	だみだこりゃ。。。	2021-12-18 07:24:37
@tomoam_mat	log4jの脆弱性、新たにCVE-2021-45105が出てきました。CVSS v3で7.5です。 修正された2.17.0がリリースされたようです。 logging.apache.org/log4j/2.x/secu…	2021-12-18 07:26:13
@jamesxujoy	@VincentMucid 又来了个CVE-2021-45105，从2.15.0修到2.16.0，再到2.17.0?	2021-12-18 07:44:15
@Myinfosecfeed	New post: "log4j 2.17.0 Released to Fix CVSS 7.5 Denial of Service (CVE-2021-45105)" ift.tt/3p33Eff	2021-12-18 07:48:43
@CoreRuleSet	#log4j is also affected by a #DoS vulnerability CVE-2021-45105. At this point, we believe our new rule and mitigati… twitter.com/i/web/status/1…	2021-12-18 08:02:26
@ohhara_shiojiri	CVE-2021-45105 CVSS 7.5 今のところはDoSだけど	2021-12-18 08:21:18
@MasafumiNegishi	Fixed in Log4j 2.17.0 (Java 8) CVE-2021-45105: Apache Log4j2 does not always protect from infinite recursion in loo… twitter.com/i/web/status/1…	2021-12-18 08:26:32
@dragonstar7722	また更新されたたかー。log4j。 CVE-2021-45105 DOSね・・・・ #log4j #vulnerability #CVE logging.apache.org/log4j/2.x/secu…	2021-12-18 08:34:45
@BWC_DE	And we're in round 3, #CVE-2021-45105 got added to the list, log4j 2.17 is the recommended version now.	2021-12-18 08:42:22
@BWC_DE	And we're in round 3, #CVE-2021-45105 got added to the list, log4j 2.17 is the recommended version now.	2021-12-18 08:43:10
@NWsecure	Ahh... It was expected. New CVE-2021-45105 is out for Log4j. logging.apache.org/log4j/2.x/secu… #log4j2 #Log4Shell	2021-12-18 08:46:24
@JoeSteel25	*updates log4j to 2.16* *CVE-2021-45105 announced* https://t.co/fMoqdiOFH4	2021-12-18 09:17:46
@hugobatista	?#log4j 2.17.0 release, fixing a 7.5 CVSS DoS vulnerability (CVE-2021-45105) "Apache Log4j2 does not always protec… twitter.com/i/web/status/1…	2021-12-18 09:23:00
@0x009AD6_810	Log4j 2.17.0 (Java 8) logging.apache.org/log4j/2.x/secu… Java 8 の Log4j 2.16.0 に DoS 脆弱性 CVE-2021-45105 (CVSS 7.5) があり修正された 2.17.0 がリリースされている	2021-12-18 09:33:51
@knqyf263	CVE-2021-45105のDoS確かにログ吐けなくなったりするけどプロセスまで落とせないな。どうやるんだろ	2021-12-18

	つやるんたら。	09:34:38
@ktgohan	logging.apache.org/log4j/2.x/secu… 風呂から出たら log4j 2.17.0 が出ていた。 CVE-2021-45105 。	2021-12-18 10:04:43
@peter_mount	Log4J 2.17.0 is now out fixing CVE-2021-45105 Yeah, there's another one, this time using recursion & not related t… twitter.com/i/web/status/1…	2021-12-18 10:05:16
@ipssignatures	The vuln CVE-2021-45105 has a tweet created 0 days ago and retweeted 12 times. twitter.com/_r_netsec/stat… #pow1rtrtwwcve	2021-12-18 10:06:00
@beingsheerazali	Apache Issues 3rd patch update -- version 2.17.0 -- to fix a new high-severity #Log4j vulnerability (CVE-2021-45105… twitter.com/i/web/status/1…	2021-12-18 10:21:26
@GossiTheDog	Log4j hype check - the latest Log4j vulnerability, todays CVE-2021-45105: - only applies to *non-default* configur… twitter.com/i/web/status/1…	2021-12-18 10:28:39
@Linda_pp	新しいの出てるな (CVE-2021-45105)	2021-12-18 10:31:33
@Ax_Sharma	NEW: CVE-2021-45105—DoS bug impacting #log4j 2.16.0, rated 'High' in severity. The recommendation now is to be on 2… twitter.com/i/web/status/1…	2021-12-18 10:33:01
@softwaremars	#software Log4j 2.17.0 released with a fix of DoS vulnerability CVE-2021-45105 [3rd bug] ift.tt/323qzOy https://t.co/0nOsCzraRT	2021-12-18 10:34:14
@NWsecure	Ahh... as expected. New CVE-2021-45105 for Log4j. One more round of fixing logging.apache.org/log4j/2.x/secu… #log4j2 #Log4Shell #CVE-2021-45105	2021-12-18 10:35:20
@MTpokerface	Apache Issues 3rd patch update -- version 2.17.0 -- to fix a new high-severity Log4j vulnerability (CVE-2021-45105)… twitter.com/i/web/status/1…	2021-12-18 10:43:03
@Stealthsploit	Still going strong. Patch your #Log4j to 2.17 which fixes CVE-2021-45105, an infinite recursion in lookups. logging.apache.org/log4j/2.x/secu…	2021-12-18 10:47:20
@sammm123	More log4j fun. CVE-2021-45105 means it's back to work. Version 2.17 here we come. *Hi-ho, Hi-ho ...."	2021-12-18 10:55:11
@_r_netsec	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5) logging.apache.org/log4j/2.x/secu…	2021-12-18 10:58:06
@CybrXx0	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5) via /r/netsec… twitter.com/i/web/status/1…	2021-12-18 10:59:30
@lm741	And bawl4j 2.17.0 has dropped with a fix for a DoS vuln (CVE-2021-45105). logging.apache.org/log4j/2.x/secu…	2021-12-18 11:05:30
@gatestone	@JuhoJauhiainen Siis 2.17 on jakelussa, mutta korjaa vain DoS-ongelman CVE-2021-45105, joka on paljon pienempi risk… twitter.com/i/web/status/1…	2021-12-18 11:22:27
@theDeallocated	In terms of updating: #log4j #CVE-2021-45046 #CVE-2021-45105 #CVE-2021-44228 https://t.co/mHFdgF1e2b	2021-12-18 11:22:36
@beingsheerazali	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5) logging.apache.org/log4j/2.x/secu…… twitter.com/i/web/status/1…	2021-12-18 11:25:40
@Jangari_nTK	また log4j の新しい脆弱性(CVE-2021-45105)出てきたのか	2021-12-18 11:30:12
@z00kov	@CERTCyberdef tracked as #CVE-2021-45105. Log4J 2.17.0 has been released.	2021-12-18 11:30:49
@MiguelHzBz	UPDATE: #log4j 2.16.0 is vulnerable, we strongly recommend updating the new version 2.17.0 to fix #CVE-2021-45105. sysdig.com/blog/exploit-d…	2021-12-18 11:34:41
@Myinfosecfeed	New post: "Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5)" ift.tt/3mgJzQS	2021-12-18 11:48:40
@Swati_THN	Apache Issues 3rd patch update -- version 2.17.0 -- to fix a new high-severity #Log4j	2021-12-18

	vulnerability (CVE-2021-45105… twitter.com/i/web/status/1…	11:49:13
@CVEreport	CVE-2021-45105 : #Apache Log4j2 versions 2.0-alpha1 through 2.16.0 excluding 2.12.3 did not protect from uncontro… twitter.com/i/web/status/1…	2021-12-18 11:57:39
@Darkarnium	Added a new rule for CVE-2021-45105 in log4j this morning, and changed the output to a file tree by default. It'll… twitter.com/i/web/status/1…	2021-12-18 12:04:05
@making	Log4j 2.16以下のバージョンに新たなDOS脆弱性(CVE-2021-45105)が見つかったため、2.17への再度アップデートが必要になりました。severityはhighでCVSS 7.5です。… twitter.com/i/web/status/1…	2021-12-18 12:12:31
@reddit_progr	Log4j 2.17.0 released with a fix of DoS vulnerability CVE-2021-45105 [3rd bug] cyberkendra.com/2021/12/3rd-vu… /post reddit.com/r/programming/…	2021-12-18 12:14:09
@ryotkak	logging.apache.org/log4j/2.x/secu… CVE-2021-45105: Apache Log4j2 does not always protect from infinite recursion in lookup evaluation	2021-12-18 12:19:57
@kojisays	いつまで続く？CVE-2021-45105 に対する Log4j 2.17.0 がリリースされましたが、Apache Solr（と Lucene も）は本件については安全とのことです。	2021-12-18 12:22:06
@arithejealous	@BashirSadjad ۲.۱۷ هم آمد :)) این هم بعدیش.	2021-12-18 12:32:08
@Takemaro_001	CVE-2021-44228に加えてCVE-2021-45046とかCVE-2021-45105が出てきて泥沼に……	2021-12-18 12:34:00
@remco_verhoef	@DIVDnl @ncsc_nl @sans_isc CORRECTION, new DoS CVE is CVE-2021-45105	2021-12-18 12:44:04
@WhiteSourceSoft	#log4j Update: CVE-2021-45105, a new vulnerability in Log4j has been published. More details and a fix suggestion c… twitter.com/i/web/status/1…	2021-12-18 12:44:07
@NandanLohitaksh	Apache Issues 3rd patch update -- version 2.17.0 -- to fix a new high-severity #Log4j vulnerability (CVE-2021-45105… twitter.com/i/web/status/1…	2021-12-18 12:46:11
@SimonByte	Latest Log4j vulnerability (CVE-2021-45105): - only affects non-default configs - could lead to a denial of servic… twitter.com/i/web/status/1…	2021-12-18 12:46:59
@thetaph1	#Apache #Solr is not vulnerable to the recently found security issues CVE-2021-45046 and CVE-2021-45105. Solr uses… twitter.com/i/web/status/1…	2021-12-18 12:49:15
@seigo303	Log4j 2.17.0がリリース。 CVE-2021-45105への対応。 ・影響範囲: 2.0-alpha1から2.16.0の ・対応策: - 2.17.0にアップグレード - 構成の変更(詳細はApacheのサイトに記… twitter.com/i/web/status/1…	2021-12-18 12:49:22
@t_nihonmatsu	12/18 #Log4j 2.17.0がリリースされました。 CVE-2021-45105 JNDIを使用するコンポーネントは、システムプロパティを介して個別に有効に サポートされているプロトコルとしてLDAPおよびLDAPSをJ… twitter.com/i/web/status/1…	2021-12-18 13:04:35
@t_nihonmatsu	セキュリティの脆弱性CVE-2021-45105 要約: Apache Log4j2 は、ルックアップ評価における無限再帰から常に保護されているわけではありません。 Apache Log4j2 バージョン 2.0-alpha1 か… twitter.com/i/web/status/1…	2021-12-18 13:05:29
@security_wang	Apache Issues 3rd patch update -- version 2.17.0 -- to fix a new high-severity #Log4j vulnerability (CVE-2021-45105… twitter.com/i/web/status/1…	2021-12-18 13:09:00
@wakatono	CVE-2021-45105（DoS脆弱性。CVSS値は 7.5）がまた1つ見つかり（lookupの無限再帰を起こすパターンが見つかった）、Log4jは2.17.0に…。Shellshockの時のbash泥沼修正の再来？ / Ap… twitter.com/i/web/status/1…	2021-12-18 13:09:07
@timdafoe	Log4j 2.17.0 released, addresses CVE-2021-45105 non-default configuration DoS: bit.ly/3DSOCgb	2021-12-18 13:17:21
/r/netsec	log4j 2.17.0 Released to Fix CVSS 7.5 Denial of Service (CVE-2021-45105)	2021-12-18 07:09:53
/r/sysadmin	Log4j - New vulnerability in 2.1.16, DOS (CVSS 7.5), CVE-2021-45105	2021-12-18 08:34:54

/r/programming	Log4j 2.17.0 released with a fix of DoS vulnerability CVE-2021-45105 [3rd bug]	2021-12-18 09:51:29
/r/apache	Log4j 2.17.0 released with a fix of DoS vulnerability CVE-2021-45105 [3rd bug]	2021-12-18 09:51:06
/r/sysadmin	Log4j UPDATE: 2.16 has a 7.5 DoS, 2.17 released	2021-12-18 09:23:05
/r/netsec	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5)	2021-12-18 10:54:02
/r/netcve	CVE-2021-45105	2021-12-18 12:38:35
/r/cybersecurity	CVE-2021-45105: Denial of Service via Uncontrolled Recursion in Log4j StrSubstitutor	2021-12-18 17:46:54
/r/ReverseEngineering	CVE-2021-45105: Denial of Service via Uncontrolled Recursion in Log4j StrSubstitutor	2021-12-18 17:42:43
/r/java	Log4j 2.17.0 released, for third CVE (CVE-2021-45105)	2021-12-18 21:01:53
/r/RedSec	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5)	2021-12-18 20:56:07
/r/u/waymapsum	Log4j version 2.17.0 fixes a new problem CVE-2021-45105 DoS vuln (CVSS score of 7.5)	2021-12-19 08:50:17
/r/pkslow	Log4j 2.17.0 released, for third CVE (CVE-2021-45105)	2021-12-19 18:19:14
/r/sysadmin	Log4jSherlock a fast PowerShell script that can scan multiple computers, made by a paranoid sysadmin.	2021-12-20 00:45:19
/r/programming	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-20 07:33:15
/r/netsec	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-20 07:32:40
/r/programminghumor	When it's monday morning and slack is already burning with log4j threads... CVE-2021-45105	2021-12-20 08:34:12
/r/selfhosted	Log4j2 nightmares for self hosters?	2021-12-21 16:54:56
/r/bag_o_news	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-21 18:04:50
/r/vulnintel	Mitigating Log4Shell and Other Log4j-Related Vulnerabilities CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	2021-12-23 10:14:43
/r/tableau	Log4j vulnerabilities in latest versions?	2022-01-10 21:51:40
/r/sysadmin	FedEx Ship Manager still has Log4j vulnerability after update.	2022-01-11 00:14:00
/r/u/detoxtechnologie	What Is Log4Shell? The Log4j Vulnerability Explained in 2022	2022-01-25 05:25:17
/r/unifi_versions	UniFi Network Application 7.0.20	2022-02-06 09:45:15
/r/PFSENSE	help: Suricata shuts down after several minutes	2022-04-09 16:21:29

← Previous ID

Next ID→