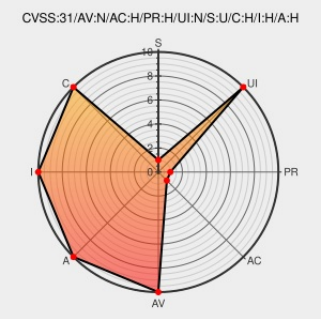
CVE-2021-44832

Published on: Not Yet Published

Last Modified on: 08/09/2022 01:24:00 AM UTC

CVE-2021-44832

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



Certain versions of Log4j from Apache contain the following vulnerability:

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

CVE-2021-44832 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.6 - MEDIUM

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

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf

[SECURITY] [DLA 2870-1] apache-log4j2 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20211229 [SECURITY] [DLA 2870-1] apache-log4j2 security update
[SECURITY] Fedora 35 Update: log4j-2.17.1-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-c6f471ce0f
CVE-2021-44832 Apache Log4j Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220104-0001/
Oracle Critical Patch Update Advisory - April 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2022.html
[SECURITY] Fedora 34 Update: log4j-2.17.1-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-1bd9151bab
Oracle Critical Patch Update Advisory - January 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2022.html
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
oss-security - CVE-2021-44832: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration	www.openwall.com text/html	MLIST [oss-security] 20211228 CVE-2021-44832: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration
[LOG4J2-3293] JDBC Appender should use JNDI Manager and JNDI access should be limited. - ASF JIRA	issues.apache.org text/html	MISC issues.apache.org/jira/browse/LOG4J2-3293
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/s1o5vlo78ypqxnzn6p8zf6t9shtq5143
Oracle Critical Patch Update Advisory - July 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujul2022.html

Related QID Numbers

178977 Debian Security Update for apache-log4j2 (DLA 2870-1)

180584 Debian Security Update for apache-log4j2 (CVE-2021-44832)

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

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

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)

282215 Fedora Security Update for log4j (FEDORA-2021-1bd9151bab)

282216 Fedora Security Update for log4j (FEDORA-2021-c6f471ce0f)

353129 Amazon Linux Security Advisory for aws-kinesis-agent : ALAS2-2022-1734

376209 Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-44832)

376210 Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) Detected Based on Qualys Log4j scan Utility (CVE-2021-44832)

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

376473 IBM Spectrum Control Multiple Vulnerabilities (6561029)

376547 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2022)

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

730362 Neo4j Database Server Affected by Apache Log4j Security Vulnerability

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)

751571 OpenSUSE Security Update for log4j (openSUSE-SU-2021:4208-1)

751576 OpenSUSE Security Update for log4j (openSUSE-SU-2022:0002-1)

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

Exploit/POC from Github

Fastest filesystem scanner for log4shell (CVE-2021-44228, CVE-2021-45046) and other vulnerable (CVE-2017-5645, CVE-20…

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	beta7	All	All
Application	Apache	Log4j	2.0	beta8	All	All
Application	Apache	Log4j	2.0	beta9	All	All
Application	Apache	Log4j	2.0	rc1	All	All
Application	Apache	Log4j	2.0	rc2	All	All
Application	Cisco	Cloudcenter	4.10.0.16	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Oracle	Communications Brm - Elastic Charging Engine	All	All	All	All
Application	Oracle	Communications Brm - Elastic Charging Engine	12.0.0.5.0	All	All	All
Application	Oracle	Communications Diameter Signaling Router	All	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 Offline Mediation Controller	All	All	All	All

Application	Oracle	Communications Offline Mediation Controller	12.0.0.5.0	All	All	All
Application	Oracle	Flexcube Private Banking	12.1.0	All	All	All
Application	Oracle	Health Sciences Data Management Workbench	2.5.2.1	All	All	All
Application	Oracle	Health Sciences Data Management Workbench	3.0.0.0	All	All	All
Application	Oracle	Health Sciences Data Management Workbench	3.1.0.3	All	All	All
Application	Oracle	Policy Automation	All	All	All	All
Application	Oracle	Policy Automation For Mobile Devices	All	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	Product Lifecycle Analytics	3.6.1	All	All	All
Application	Oracle	Retail Assortment Planning	16.0.3	All	All	All
Application	Oracle	Retail Fiscal Management	14.2	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 Xstore Point Of Service	17.0.4	All	All	All
Application	Oracle	Retail Xstore Point Of Service	18.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	19.0.2	All	All	All
Application	Oracle	Retail Xstore Point Of Service	20.0.1	All	All	All
Application	Oracle	Retail Xstore Point Of Service	21.0.1	All	All	All
Application	Oracle	Siebel Ui Framework	21.12	All	All	All
Application	Oracle	Siebel Ui Framework	All	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

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

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

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

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

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:rc2:*:*:*:*:*:*:

cpe:2.3:a:cisco:cloudcenter:4.10.0.16:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_brm_-_elastic_charging_engine:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_brm_-_elastic_charging_engine:12.0.0.5.0:*:*:*:*:*:*:*:

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

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_offline_mediation_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_offline_mediation_controller:12.0.0.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:flexcube_private_banking:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_data_management_workbench:2.5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_data_management_workbench:3.0.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:health_sciences_data_management_workbench:3.1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:policy_automation:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:policy_automation_for_mobile_devices:*:*:*:*:*:*:*:*:

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:product_lifecycle_analytics:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_assortment_planning:16.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_fiscal_management:14.2:*:*:*:*:*:*:*:

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_xstore_point_of_service:17.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_xstore_point_of_service:18.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_xstore_point_of_service:19.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_xstore_point_of_service:20.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:retail_xstore_point_of_service:21.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:siebel_ui_framework:21.12:*:*:*:*:*:*:*:

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

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@marcwrogers	@douglasmun @GossiTheDog Looks like log4j CVE-2021-44832 has non default preconditions: “You are loading configura… twitter.com/i/web/status/1…	2021-12-28 16:54:04
@sherlocksecure	New #log4j 2.17.0 RCE may be assigned as CVE-2021-44832 #CVE-2021-44832 Vulnerability confirmed!!! #bugbounty #cybersecurity #apache	2021-12-28 17:02:10
@hmier	@vbramosa CVE-2021-44832	2021-12-28

@himiel	@vhiramosa CVE-2021-44832	2021-12-28 17:13:08
@sherlocksecure	Disclosure is in progress! @YNizry check Marx SCA tool can detect this vulnerability now!! #CVE-2021-44832 #Log4j… twitter.com/i/web/status/1…	2021-12-28 17:22:52
@ofaltundal	Wait for it CVE-2021-44832 #cybersecurity #Log4j	2021-12-28 17:24:35
@vxunderground	CVE-2021-44832 https://t.co/5eoFum3s0s	2021-12-28 17:46:46
@thechrisharrod	Here we go again...	2021-12-28 17:50:06
@JulianNorton	@vxunderground No link in NIST yet	2021-12-28 17:52:40
@Orwell84_	CVE-2021-44832 be like... #log4j https://t.co/LfQD5iRSw1	2021-12-28 17:54:37
@B3n_5mash	@GossiTheDog @marcwrogers @douglasmun	2021-12-28 18:03:42
@OguzhanTopgul	Another vulnerability in #log4j2 that is also affecting version 2.17.0. CVE-2021-44832 Successful exploitation req… twitter.com/i/web/status/1…	2021-12-28 18:14:21
@__kokumoto	訳）バージョン2.17.0にも影響する、log4j2における更なる脆弱性。 CVE-2021-44832 悪用成功のためにはリモートサーバから読み込まれている構成ファイルの乗っ取り/変更を行う必要がある 詳細と公式開示はまだこ… twitter.com/i/web/status/1…	2021-12-28 18:22:44
@syndrowm	Welp... CVE-2021-44832 #log4j #long4j https://t.co/mt6QScDhrL	2021-12-28 18:26:15
@jan_karel	CVE-2021-44832 is niet alleen JDBC.	2021-12-28 18:41:21
@hasan_zmzm	@log4j_0day @vxunderground Not yet, here says nothing:	2021-12-28 18:50:33
@wdormann	If any person or organization is suggesting you get spun up about CVE-2021-44832, you should really take a good loo… twitter.com/i/web/status/1…	2021-12-28 18:55:39
@sheikhrishad0	CVE-2021-44832 ? #log4j #bugbounty	2021-12-28 19:17:56
@jschauma	logging.apache.org/log4j/2.x/secu… now has the latest information: CVE-2021-44832 CVSS: 6.6 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/… twitter.com/i/web/status/1…	2021-12-28 19:23:47
@wdormann	@attritionorg 1) Search github for CVE-2021-44832 github.com/search?q=%22CV… 2) Find repo that is likely the log4j sta… twitter.com/i/web/status/1…	2021-12-28 19:25:42
@skoops	CVE-2021-44832 Apache Log4j 2 RCE Hi again. https://t.co/Rgl4HgK8xm	2021-12-28 19:29:50
@41thexplorer	CVE-2021-44832, the new #log4j RCE vulnerability is official. It's CVSS score is 6.6 as the exploitation complexit… twitter.com/i/web/status/1…	2021-12-28 19:30:01
@marcwrogers	Details on log4j CVE-2021-44832 live now: logging.apache.org/log4j/2.x/inde… as stated before non default preconditions reduce risk in most cases.	2021-12-28 19:30:48
@cbirajdar22	Okay so it is official now, new #log4j RCE found and published as CVE-2021-44832. IMPORTANT TO NOTE: Attack Compl… twitter.com/i/web/status/1…	2021-12-28 19:31:01
@aiacobelli_sec	@wdormann -> there is no formal CVE, this could be a scam! I've read the 2.17.1 diff and I'… twitter.com/i/web/status/1…	2021-12-28 19:31:23
@jschauma	Looks like issues.apache.org/jira/browse/LO… is the ticket for CVE-2021-44832 that's about to be backfilled.	2021-12-28 19:32:06

@41thexplorer	CVE-2021-44832 is fixed in log4j 2.17.1 (Java 8). It looks like log4j 2.12.4 and 2.3.2 (Java 7 and 6) are coming soon.	2021-12-28 19:32:47
@netalexx	Details on log4j CVE-2021-44832 live now logging.apache.org/log4j/2.x/inde…	2021-12-28 19:34:25
@GaryGregory	The #log4j team has released 2.17.1 to address CVE-2021-44832 (severity: moderate) where an attacker can cause an R… twitter.com/i/web/status/1…	2021-12-28 19:34:35
@XenoPhage	@YNizry And the new CVE (CVE-2021-44832) is out, along with an updated 2.17.1 log4j.. It's an RCE, but in a non-def… twitter.com/i/web/status/1…	2021-12-28 20:12:14
@SeguInfo	#Log4Shell Nueva actualización publicada #Log4j 2.17.1 (Java8), 2.12.4 (Java7), 2.3.2 (Java6) CVE-2021-44832 (6.6 M… twitter.com/i/web/status/1…	2021-12-28 20:12:14
@entelCybersec	? No se podía terminar el año sin una nueva #vulnerabilidad de #log4j ? ⚠Se le ha asignado el CVE-2021-44832 con… twitter.com/i/web/status/1…	2021-12-28 20:15:47
@_hillu	@isotopp Heuristik muss nicht in die Wartung. Gut! CVE-2021-44832: "vulnerable to a remote code execution (RCE) at… twitter.com/i/web/status/1…	2021-12-28 20:15:53
@Ax_Sharma	It's official. #log4j 2.17.1 is OUT fixing a 'Moderate' severity RCE, tracked as CVE-2021-44832. This marks the 5th… twitter.com/i/web/status/1…	2021-12-28 20:16:13
@eudyzerpa	#Log4Shell Nueva actualización publicada #Log4j 2.17.1 (Java8), 2.12.4 (Java7), 2.3.2 (Java6) CVE-2021-44832 (6.6 M… twitter.com/i/web/status/1…	2021-12-28 20:18:20
@wagde	@YNizry Here we go: Happy New CVE CVE-2021-44832 logging.apache.org/log4j/2.x/secu…	2021-12-28 20:18:43
@wagde	Happy New CVE CVE-2021-44832 #log4j	2021-12-28 20:19:26
@seolsson	@pwntester If it's about CVE-2021-44832 fixed in 2.17.1 it looks like nothing. Don't know if it's the same issue, but seems likely.	2021-12-28 20:21:59
@zmanion	This (CVE-2021-44832), and more importantly CVE-2021-44228 (the one that matters), were expensive coordinated vulne… twitter.com/i/web/status/1…	2021-12-28 20:28:50
@cyb3rops	Log4j 2.17 RCE CVE-2021-44832 in a nutshell https://t.co/GPaHcDHlj0	2021-12-28 20:32:15
@seolsson	Re log4j 2.17.1: So far CVE-2021-44832 looks like a non-issue in most cases. At least not the most urgent thing to… twitter.com/i/web/status/1…	2021-12-28 20:37:26
@ennozdd	CVE-2021-44832 is another log4j RCE vulnerability. However, you need to have access to the configuration file to ex… twitter.com/i/web/status/1…	2021-12-28 20:46:00
@basalberts	Seems a little much to pre-hype CVE-2021-44832 as an RCE with a teaser screenshot considering how many folks will b… twitter.com/i/web/status/1…	2021-12-28 20:46:57
@nofars	Fourth time's the charm? #log4j	2021-12-28 20:48:40
@CroodSolutions	Can we just officially start calling this log-nightmare now?	2021-12-28 21:00:19
@TorryCrass	And again, an new 0-day RCE for #log4j affecting latest v2.17 update (CVE-2021-44832) put in 2 hours ago and fix v2… twitter.com/i/web/status/1…	2021-12-28 21:02:50
@Myinfosecfeed	New post: "New Log4j CVE - CVE-2021-44832. Another JNDI RCE. Fixed in latest release." ift.tt/3JmSc6h	2021-12-28 21:48:11
@knqyf263	攻撃者が設定のjndiName変えられる権限がある場合に影響ありってことかな。風邪でダウンしていてちゃんと読めてないけど。 checkmarx.com/blog/cve-2021-…	2021-12-28 21:49:37
/r/netsecstudents	CVE-2021-44832: A Medium Severity Was Found in Log4j	2022-01-10 08:25:49

/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/PFSENSE	help: Suricata shuts down after several minutes	2022-04-09 16:21:29
/r/QRadar	How after this long????????? Due to use of Apache Log4j, IBM QRadar SIEM is affected by arbitrary code execution	2022-10-27 14:25:03

← Previous ID

Next ID→