



CVE-2021-4104

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-4104
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-14 12:15:00 UTC
Updated	2023-12-22 09:15:00 UTC
Description	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Langu
Application	Apache	Log4j	1.2	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Oracle	Advanced Supply Chain Planning	12.1	All	All	All
Application	Oracle	Advanced Supply Chain Planning	12.2	All	All	All
Application	Oracle	Business Intelligence	12.2.1.3.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.4.0	All	All	All
Application	Oracle	Business Intelligence	5.9.0.0.0	All	All	All
Application	Oracle	Business Process Management Suite	12.2.1.3.0	All	All	All
Application	Oracle	Business Process Management Suite	12.2.1.4.0	All	All	All
Application	Oracle	Communications Eagle Ftp Table Base Retrieval	4.5	All	All	All
Application	Oracle	Communications Messaging Server	8.1	All	All	All
Application	Oracle	Communications Network Integrity	7.3.6	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	Communications Unified Inventory Management	7.3.4	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	E-business Suite Cloud Manager And Cloud Backup Module	2.2.1.1.1	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	Financial Services Revenue Management And Billing Analytics	2.7.0.0	All	All	All
Application	Oracle	Financial Services Revenue Management And Billing Analytics	2.7.0.1	All	All	All
Application	Oracle	Financial Services Revenue Management And Billing Analytics	2.8.0.0	All	All	All
Application	Oracle	Fusion Middleware Common Libraries And Tools	12.2.1.4.0	All	All	All
Application	Oracle	Goldengate	-	All	All	All
Application	Oracle	Healthcare Data Repository	8.1.0	All	All	All
Application	Oracle	Hyperion Data Relationship Management	All	All	All	All
Application	Oracle	Hyperion Infrastructure Technology	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	Jdeveloper	12.2.1.3.0	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Retail Allocation	14.1.3.2	All	All	All
Application	Oracle	Retail Allocation	15.0.3.1	All	All	All
Application	Oracle	Retail Allocation	16.0.3	All	All	All
Application	Oracle	Retail Allocation	19.0.1	All	All	All
Application	Oracle	Retail Extract Transform And Load	13.2.5	All	All	All
Application	Oracle	Stream Analytics	-	All	All	All
Application	Oracle	Timesten Grid	-	All	All	All
Application	Oracle	Tuxedo	12.2.2.0.0	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.1.1	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.2.2	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.3.1	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
Application	Redhat	Codeready Studio	12.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Integration Camel K	-	All	All	All

Application	Redhat	Integration Camel Quarkus	-	All	All	All
Application	Redhat	Jboss A-mq	6.0.0	All	All	All
Application	Redhat	Jboss A-mq	7	All	All	All
Application	Redhat	Jboss A-mq Streaming	-	All	All	All
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Data Virtualization	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0	All	All	All
Application	Redhat	Jboss Fuse	6.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Jboss Fuse Service Works	6.0	All	All	All
Application	Redhat	Jboss Operations Network	3.0	All	All	All
Application	Redhat	Jboss Web Server	3.0	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Openshift Container Platform	4.6	All	All	All
Application	Redhat	Openshift Container Platform	4.7	All	All	All
Application	Redhat	Openshift Container Platform	4.8	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Software Collections	-	All	All	All

References

Reference	Source	Link
Restrict LDAP access via JNDI by rgoers · Pull Request #608 · apache/logging-log4j2 · GitHub	MISC	github.com
CVE-2021-4104 Apache Log4j Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Red Hat Customer Portal - Access to 24x7 support and knowledge		access.redhat.com
Security Advisory		psirt.global.sonicwall.com
oss-security - CVE-2022-23302: Deserialization of untrusted data in JMSSink in Apache Log4j 1.x	MLIST	www.openwall.com
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com
cve-website		www.cve.org
Oracle Critical Patch Update Advisory - April 2022		www.oracle.com
Minecraft Server: Remote Code Execution (GLSA 202312-02) — Gentoo security		security.gentoo.org
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com
Arduino: Remote Code Execution (GLSA 202312-04) — Gentoo security		security.gentoo.org
IBM Spectrum Protect: Multiple Vulnerabilities (GLSA 202209-02) — Gentoo security	GENTOO	security.gentoo.org

Ubiquiti UniFi: remote code execution via bundled log4j (GLSA 202310-16) — Gentoo security		security.gentoo.org
VU#930724 - Apache Log4j allows insecure JNDI lookups	CERT-VN	www.kb.cert.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159573 Oracle Enterprise Linux Security Update for log4j (ELSA-2021-5206)
159603 Oracle Enterprise Linux Security Update for parfait:0.5 (ELSA-2022-0290)
159619 Oracle Enterprise Linux Security Update for log4j (ELSA-2022-9056)
179047 Debian Security Update for apache-log4j1.2 (DLA 2905-1)
179633 Debian Security Update for apache-log4j1.2 (CVE-2021-4104)
198633 Ubuntu Security Notification for Apache Log4j 1.2 Vulnerability (USN-5223-1)
20251 IBM DB2 Security Update for Log4j (6528678)
239973 Red Hat Update for log4j (RHSA-2021:5206)
239980 Red Hat Update for rh-maven36-log4j12 (RHSA-2021:5269)
240034 Red Hat Update for parfait:0.5 (RHSA-2022:0289)
240035 Red Hat Update for parfait:0.5 (RHSA-2022:0290)
240036 Red Hat Update for parfait:0.5 (RHSA-2022:0291)
240059 Red Hat Update for JBoss Enterprise Application Platform 7.4 (RHSA-2022:0436)
240060 Red Hat Update for JBoss Enterprise Application Platform 6.4 (RHSA-2022:0438)
240078 Red Hat Update for red hat jboss web server 3.1 service pack 14 (RHSA-2022:0524)
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)
240452 Red Hat Update for parfait:0.5 (RHSA-2022:0294)
240508 Red Hat Update for JBoss Enterprise Application Platform 6.4.2 (RHSA-2022:5459)
240511 Red Hat Update for JBoss Enterprise Application Platform 6.4.2 (RHSA-2022:5460)
257136 CentOS Security Update for log4j (CESA-2021:5206)
353112 Amazon Linux Security Advisory for log4j : ALAS-2022-1562

353124 Amazon Linux Security Advisory for log4j : ALAS2-2022-1739
376187 Apache Log4j 1.2 Remote Code Execution Vulnerability
376415 IBM WebSphere Application Server Multiple Vulnerabilities (Log4Shell) (6526750)
376425 Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (Log4Shell) (Doc_ID_2817011.1)
377147 Alibaba Cloud Linux Security Update for parfait:0.5 (ALINUX3-SA-2022:0006)
377225 Alibaba Cloud Linux Security Update for log4j (ALINUX2-SA-2021:0072)
671353 EulerOS Security Update for log4j (EulerOS-SA-2022-1276)
710616 Gentoo Linux IBM Spectrum Protect Multiple Vulnerabilities (GLSA 202209-02)
710775 Gentoo Linux Ubiquiti UniFi Remote Code Execution (RCE) via bundled log4j Vulnerability (GLSA 202310-16)
710804 Gentoo Linux Minecraft Server Remote Code Execution (RCE) Vulnerability (GLSA 202312-02)
710807 Gentoo Linux Arduino Remote Code Execution (RCE) Vulnerability (GLSA 202312-04)
730566 Atlassian Jira Server and Data Center Log4j Vulnerability (JRASERVER-73885)
751522 SUSE Enterprise Linux Security Update for log4j (SUSE-SU-2021:4111-1)
751523 SUSE Enterprise Linux Security Update for log4j (SUSE-SU-2021:4115-1)
751524 OpenSUSE Security Update for log4j12 (openSUSE-SU-2021:4112-1)
751525 OpenSUSE Security Update for log4j (openSUSE-SU-2021:4111-1)
751556 OpenSUSE Security Update for log4j12 (openSUSE-SU-2021:1612-1)
87483 Oracle WebLogic Server Multiple Vulnerabilities (Log4Shell) (Doc_ID_2817011.1)
940440 AlmaLinux Security Update for parfait:0.5 (ALSA-2022:0290)
960689 Rocky Linux Security Update for parfait:0.5 (RLSA-2022:0290)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)