



CVE-2021-36374

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-36374
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-14 07:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amo

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ant	All	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	Banking Trade Finance	14.5	All	All	All
Application	Oracle	Banking Treasury Management	14.5	All	All	All
Application	Oracle	Communications Cloud Native Core Automated Test Suite	1.9.0	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	1.11.0	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	All	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	All	All	All	All
Application	Oracle	Communications Order And Service Management	7.3	All	All	All
Application	Oracle	Communications Order And Service Management	7.4	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.3.0	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.0	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 Unified Inventory Management	7.5.0	All	All	All
Application	Oracle	Enterprise Repository	11.1.1.7.0	All	All	All

Application	Oracle	Financial Services Analytical Applications Infrastructure	All	All	All	All
Application	Oracle	Health Sciences Information Manager	3.0.0.1	All	All	All
Application	Oracle	Health Sciences Information Manager	All	All	All	All
Application	Oracle	Insurance Policy Administration	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 Gateway	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	All	All	All	All
Application	Oracle	Product Lifecycle Analytics	3.6.1	All	All	All
Application	Oracle	Real-time Decision Server	11.1.1.9.0	All	All	All
Application	Oracle	Real-time Decision Server	3.2.0.0	All	All	All
Application	Oracle	Retail Advanced Inventory Planning	14.1	All	All	All
Application	Oracle	Retail Advanced Inventory Planning	15.0	All	All	All
Application	Oracle	Retail Advanced Inventory Planning	16.0	All	All	All
Application	Oracle	Retail Back Office	14.0	All	All	All
Application	Oracle	Retail Back Office	14.1	All	All	All
Application	Oracle	Retail Bulk Data Integration	16.0.3.0	All	All	All
Application	Oracle	Retail Bulk Data Integration	19.0.1	All	All	All
Application	Oracle	Retail Central Office	14.0	All	All	All
Application	Oracle	Retail Central Office	14.1	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 Extract Transform And Load	13.2.8	All	All	All
Application	Oracle	Retail Financial Integration	14.1.3.2	All	All	All
Application	Oracle	Retail Financial Integration	15.0.4.0	All	All	All
Application	Oracle	Retail Financial Integration	16.0.3.0	All	All	All
Application	Oracle	Retail Integration Bus	14.1.3.2	All	All	All
Application	Oracle	Retail Integration Bus	15.0.4.0	All	All	All
Application	Oracle	Retail Integration Bus	16.0.3.0	All	All	All
Application	Oracle	Retail Integration Bus	19.0.1.0	All	All	All
Application	Oracle	Retail Invoice Matching	16.0.3	All	All	All

Application	Oracle	Retail Merchandising System	19.0.1	All	All	All
Application	Oracle	Retail Point-of-service	14.0	All	All	All
Application	Oracle	Retail Point-of-service	14.1	All	All	All
Application	Oracle	Retail Predictive Application Server	14.1.3	All	All	All
Application	Oracle	Retail Predictive Application Server	15.0.3	All	All	All
Application	Oracle	Retail Predictive Application Server	16.0.3.0	All	All	All
Application	Oracle	Retail Service Backbone	14.1.3.2	All	All	All
Application	Oracle	Retail Service Backbone	15.0.4.0	All	All	All
Application	Oracle	Retail Service Backbone	16.0.3.0	All	All	All
Application	Oracle	Retail Service Backbone	19.0.1.0	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0	All	All	All
Application	Oracle	Retail Store Inventory Management	16.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0.6	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	Timesten In-memory Database	All	All	All	All
Application	Oracle	Utilities Framework	4.2.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.2.0.3.0	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	Utilities Testing Accelerator	6.0.0.1.1	All	All	All

References

Reference

Apache Ant - Apache Ant Security Reports

[groovy-notifications] 20210715 [jira] [Resolved] (GROOVY-10169) Bump Ant version to 1.10.11 (incorporates CVE-2021-36373 and CVE-2021-36374)
lists.apache.org/thread.html/rdd5412a5b9a25aed2a02c3317052d38a97128314d50bc1ed...

Oracle Critical Patch Update Advisory - April 2022

July 2021 Apache Ant Vulnerabilities in NetApp Products | NetApp Product Security

Pony Mail!

Oracle Critical Patch Update Advisory - October 2021

[groovy-commits] 20210715 [groovy] 02/07: GROOVY-10169: Bump Ant version to 1.10.11 (incorporates CVE-2021-36373 and CVE-2021-36

Oracle Critical Patch Update Advisory - January 2022

[groovy-commits] 20210714 [groovy] 08/09: GROOVY-10169: Bump Ant version to 1.10.11 (incorporates CVE-2021-36373 and CVE-2021-36

Pony Mail!

Pony Mail!

[myfaces-dev] 20210830 [GitHub] [myfaces-tobago] lofwyr14 opened a new pull request #1215: build: CVE fix

Pony Mail!

Oracle Critical Patch Update Advisory - July 2022

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Discovery Credit

LEGACY: This issue is similar to <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36090> present in Apache Commons Compress which has been detected by OSS Fuzz.

Legacy QID Mappings

150735 Oracle WebLogic Server Multiple Vulnerabilities (CPU - OCT2023)
182126 Debian Security Update for ant (CVE-2021-36374)
296065 Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)
354116 Amazon Linux Security Advisory for ant : ALAS2-2022-1880
376123 IBM Installation Manager Multiple Vulnerabilities
501805 Alpine Linux Security Update for apache-ant
504580 Alpine Linux Security Update for apache-ant
670695 EulerOS Security Update for ant (EulerOS-SA-2021-2453)
670958 EulerOS Security Update for ant (EulerOS-SA-2021-2651)
671660 EulerOS Security Update for ant (EulerOS-SA-2022-1703)
752076 SUSE Enterprise Linux Security Update for ant (SUSE-SU-2022:1417-1)
753206 SUSE Enterprise Linux Security Update for ant (SUSE-SU-2022:1418-1)
87548 Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2023)
900240 CBL-Mariner Linux Security Update for ant 1.10.9
900240 CBL-Mariner Linux Security Update for ant 1.10.9

[903404](#) Common Base Linux Mariner (CBL-Mariner) Security Update for ant (4438)

[980362](#) Java (maven) Security Update for org.apache.ant:ant (GHSA-5v34-g2px-j4fw)

© [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](#).

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