



CVE-2022-25647

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

Summary

CVE	CVE-2022-25647
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-01 16:15:00 UTC
Updated	2022-11-28 17:33:00 UTC
Description	The package com.google.code.gson:gson before 2.8.9 are vulnerable to Deserialization of Untrusted Data via the writeRep

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Google	Gson	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Oracle	Financial Services Crime And Compliance Management Studio	8.0.8.2.0	All	All	All
Application	Oracle	Financial Services Crime And Compliance Management Studio	8.0.8.3.0	All	All	All
Application	Oracle	Graalvm	20.3.6	All	All	All
Application	Oracle	Graalvm	21.3.2	All	All	All
Application	Oracle	Graalvm	22.1.0	All	All	All
Application	Oracle	Retail Order Broker	18.0	All	All	All
Application	Oracle	Retail Order Broker	19.1	All	All	All

References

Reference	Source	Link
-----------	--------	------

Deserialization of Untrusted Data in com.google.code.gson:gson Snyk	MISC	snyk.io
[SECURITY] [DLA 3100-1] libgoogle-gson-java security update	MLIST	lists.debian.org
Debian -- Security Information -- DSA-5227-1 libgoogle-gson-java	DEBIAN	www.debian.org
Prevent Java deserialization of internal classes by Marcono1234 · Pull Request #1991 · google/gson · GitHub	MISC	github.com
Prevent Java deserialization of internal classes by Marcono1234 · Pull Request #1991 · google/gson · GitHub	MISC	github.com
CVE-2022-25647 Google Gson Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com
[SECURITY] [DLA 3001-1] libgoogle-gson-java security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Marcono1234

Legacy QID Mappings

179282 Debian Security Update for libgoogle-gson-java (DLA 3001-1)
180999 Debian Security Update for libgoogle-gson-java (DLA 3100-1)
181000 Debian Security Update for libgoogle-gson-java (DSA 5227-1)
184703 Debian Security Update for libgoogle-gson-java (CVE-2022-25647)
200185 Ubuntu Security Notification for Gson Vulnerability (USN-6692-1)
20270 Oracle Database 21c Critical Patch Update - October 2022
20271 Oracle Database 19c Critical Patch Update - October 2022
20272 Oracle Database 19c Critical OJVM Patch Update - October 2022
240589 Red Hat Update for JBoss Enterprise Application Platform 7.4.6 (RHSA-2022:5893)
240590 Red Hat Update for JBoss Enterprise Application Platform 7.4.6 (RHSA-2022:5892)
240591 Red Hat Update for red hat jboss enterprise application platform 7.4.6 (RHSA-2022:5894)
376941 F5 BIG-IP Gson Denial of Service (DoS) Vulnerability (K00994461)
377645 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUOCT2022)
378991 Atlassian Jira Service Management Server and Data Center Critical Severity Authentication Vulnerability (JSDSERVER-14007)
502455 Alpine Linux Security Update for openjdk15

502456 Alpine Linux Security Update for openjdk17
502468 Alpine Linux Security Update for openjdk11
502484 Alpine Linux Security Update for openjdk13
502578 Alpine Linux Security Update for openjdk11
752220 SUSE Enterprise Linux Security Update for google-gson (SUSE-SU-2022:2044-1)
87530 Oracle WebLogic Server Multiple Vulnerabilities (CPUJAN2023)

© [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](#)