



# CVE-2018-10237

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

## Summary

<b>CVE</b>	CVE-2018-10237
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-26 21:29:00 UTC
<b>Updated</b>	2023-11-07 02:51:00 UTC
<b>Description</b>	Unbounded memory allocation in Google Guava 11.0 through 24.x before 24.1.1 allows remote attackers to conduct denial

## Risk And Classification

### Problem Types: CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Guava	All	All	All	All
Application	Google	Guava	All	All	All	All
Application	Oracle	Banking Payments	All	All	All	All
Application	Oracle	Communications Ip Service Activator	7.3.0	All	All	All
Application	Oracle	Communications Ip Service Activator	7.4.0	All	All	All
Application	Oracle	Customer Management And Segmentation Foundation	18.0	All	All	All
Application	Oracle	Database Server	12.2.0.1	All	All	All
Application	Oracle	Database Server	18c	All	All	All
Application	Oracle	Database Server	19c	All	All	All
Application	Oracle	Flexcube Investor Servicing	12.1.0	All	All	All
Application	Oracle	Flexcube Investor Servicing	12.3.0	All	All	All
Application	Oracle	Flexcube Investor Servicing	12.4.0	All	All	All
Application	Oracle	Flexcube Investor Servicing	14.0.0	All	All	All
Application	Oracle	Flexcube Investor Servicing	14.1.0	All	All	All
Application	Oracle	Flexcube Private Banking	12.0.0	All	All	All
Application	Oracle	Flexcube Private Banking	12.1.0	All	All	All
Application	Oracle	Retail Integration Bus	15.0	All	All	All

Application	Oracle	Retail Integration Bus	16.0	All	All	All
Application	Oracle	Retail Integration Bus	15.0	All	All	All
Application	Oracle	Retail Integration Bus	16.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	15.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Retail Xstore Point Of Service	15.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Satellite	6.4	All	All	All
Application	Redhat	Satellite	6.4	All	All	All
Application	Redhat	Satellite Capsule	6.4	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

Application	Redhat	Virtualization	4.2	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.2	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

## References

Reference
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
CVE-2018-10237 Guava Vulnerability in NetApp Products   NetApp Product Security
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - July 2020
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Google Groups
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat JBoss EAP Component Errors Let Remote Users Deny Service and Remote Authenticated Users Gain Potentially Sensitive Informati

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Oracle Critical Patch Update Advisory - October 2021

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - April 2020
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - January 2021
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
[arrow-github] 20210610 [GitHub] [arrow] projjal opened a new pull request #10501: ARROW-13032: Update guava version
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings
<a href="#">378883</a> Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
<a href="#">87467</a> Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2021)
<a href="#">980284</a> Java (maven) Security Update for com.google.guava:guava (GHSA-mvr2-9pj6-7w5j)

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](#)**