



# CVE-2017-3533

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2017-3533   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert_us@oracle.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2017-04-24 19:59:00 UTC   |
| <b>Updated</b>         | 2022-05-13 14:52:00 UTC   |
| <b>Description</b>     | Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Sup |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version  | Update     | Edition | Language |
|------------------|------------------------|------------------------------|----------|------------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0      | All        | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0      | All        | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.6.0    | update141  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.6.0    | update_141 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.7.0    | update131  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.8.0    | update121  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.6.0    | update_141 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.7.0    | update131  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jdk</a>          | 1.8.0    | update121  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.6.0    | update141  | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.6.0    | update_141 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.7.0    | update_131 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.8.0    | update_121 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.6.0    | update_141 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.7.0    | update_131 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jre</a>          | 1.8.0    | update_121 | All     | All      |
| Application      | <a href="#">Oracle</a> | <a href="#">Jrockit</a>      | r28.3.13 | All        | All     | All      |

|                  |        |                              |          |     |     |     |
|------------------|--------|------------------------------|----------|-----|-----|-----|
| Application      | Oracle | Jrockit                      | r28.3.13 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop     | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop     | 7.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop     | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop     | 7.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server      | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server      | 7.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server      | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server      | 7.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.4      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.4      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.4      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.5      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.4      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.5      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus  | 7.3      | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus  | 7.6      | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0      | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0      | All | All | All |
| Application      | Redhat | Icedtea                      | All      | All | All | All |
| Application      | Redhat | Icedtea                      | All      | All | All | All |
| Application      | Redhat | Satellite                    | 5.8      | All | All | All |
| Application      | Redhat | Satellite                    | 5.8      | All | All | All |

## References

### Reference

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Oracle Critical Patch Update - April 2017](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Oracle Java SE and JRockit CVE-2017-3533 Remote Security Vulnerability](#)

[Red Hat Customer Portal](#)

[Debian -- Security Information -- DSA-3858-1 openjdk-7](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Oracle JDK/JRE: Multiple vulnerabilities \(GLSA 201705-03\) — Gentoo security](#)

[IcedTea: Multiple vulnerabilities \(GLSA 201707-01\) — Gentoo security](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Oracle Java SE Bugs Let Remote Users Access and Modify Data, Deny Service, and Gain Elevated Privileges and Remote and Local Users C](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[376056](#) IBM Cognos Analytics Multiple Vulnerabilities (566643)

[378136](#) Virtuozzo Linux Security Update for java-1.8.0-openjdk-debug (VZLSA-2017:1109)

[378171](#) Virtuozzo Linux Security Update for java-1.8.0-openjdk-javadoc-zip (VZLSA-2017:1108)

[378231](#) Virtuozzo Linux Security Update for java-1.7.0-openjdk-demo (VZLSA-2017:1204)

[710327](#) Gentoo Linux Oracle Java Development Toolkit/Java Runtime Error Multiple Vulnerabilities (GLSA 201705-03)

[710425](#) Gentoo Linux IcedTea Multiple Vulnerabilities (GLSA 201707-01)

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](https://status.cve.report)**