



# CVE-2016-5597

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2016-5597  |
| <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>       | 2016-10-25 14:31:00 UTC  |
| <b>Updated</b>         | 2022-05-13 14:57:00 UTC  |
| <b>Description</b>     | Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to |

## Risk And Classification

**Problem Types: CWE-200**

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product             | Version | Update     | Edition | Language |
|-------------|------------------------|---------------------|---------|------------|---------|----------|
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.6.0   | update121  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.6.0   | update_121 | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.7.0   | update111  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.8.0   | update101  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.8.0   | update102  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.6.0   | update_121 | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.7.0   | update111  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.8.0   | update101  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jdk</a> | 1.8.0   | update102  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.6.0   | update121  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.6.0   | update_121 | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.7.0   | update111  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.7.0   | update_111 | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0   | update101  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0   | update102  | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0   | update_101 | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0   | update_102 | All     | All      |

|             |                        |                     |       |            |     |     |
|-------------|------------------------|---------------------|-------|------------|-----|-----|
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.6.0 | update_121 | All | All |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.7.0 | update_111 | All | All |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0 | update_101 | All | All |
| Application | <a href="#">Oracle</a> | <a href="#">Jre</a> | 1.8.0 | update_102 | All | All |

## References

| Reference   | Source          |
|---|-----------------|
| Red Hat Customer Portal   | REDHAT          |
| USN-3154-1: OpenJDK 6 vulnerabilities   Ubuntu  | UBUNTU          |
| Red Hat Customer Portal   | REDHAT          |
| IcedTea: Multiple vulnerabilities (GLSA 201701-43) — Gentoo security  | GENTOO          |
| Red Hat Customer Portal   | REDHAT          |
| Oracle Java SE Multiple Flaws Let Remote Users Access Data, Partially Modify Data, and Gain Elevated Privileges - SecurityTracker | SECURITYTRACKER |
| October 2016 Java Platform Standard Edition Vulnerabilities in Multiple NetApp Products   NetApp Product Security                 | CONFIRMED       |
| Red Hat Customer Portal   | REDHAT          |
| Debian -- Security Information -- DSA-3707-1 openjdk-7  | DEBIAN          |
| USN-3130-1: OpenJDK 7 vulnerabilities   Ubuntu  | UBUNTU          |
| Oracle Critical Patch Update - October 2016   | CONFIRMED       |
| Red Hat Customer Portal   | REDHAT          |
| Oracle Java SE CVE-2016-5597 Remote Security Vulnerability  | BID             |
| Red Hat Customer Portal   | REDHAT          |
| Red Hat Customer Portal   | REDHAT          |
| Red Hat Customer Portal   | REDHAT          |
| Red Hat Customer Portal   | REDHAT          |
| Red Hat Customer Portal   | REDHAT          |
| Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201611-04) — Gentoo security   | GENTOO          |
| Red Hat Customer Portal   | REDHAT          |
| Red Hat Customer Portal   | REDHAT          |
| CVE Program record  | CVE.COM         |
| NVD vulnerability detail  | NVD             |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|   |
|---|
| <a href="#">376056</a> IBM Cognos Analytics Multiple Vulnerabilities (566643)                           |
| <a href="#">378293</a> Virtuozzo Linux Security Update for java-1.6.0-openjdk-javadoc (VZLSA-2017:0061) |

© [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](#)**