



# CVE-2010-3567

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-3567                                                                                                            |
| <b>State</b>           | PUBLISHED                                                                                                                |
| <b>Assigner</b>        | oracle                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2010-10-19 22:00:03 UTC                                                                                                  |
| <b>Updated</b>         | 2026-04-29 01:13:23 UTC                                                                                                  |
| <b>Description</b>     | Unspecified vulnerability in the 2D component in Oracle Java SE and Java for Business 6 Update 21, and 5.0 Update 25 all |

## Risk And Classification

**Primary CVSS:** v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

**Problem Types:** NVD-CWE-noinfo | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Sun    | Jdk     | 1.5.0   | All    | All     | All      |

|             |     |     |       |             |     |     |
|-------------|-----|-----|-------|-------------|-----|-----|
| Application | Sun | Jdk | 1.5.0 | update1     | All | All |
| Application | Sun | Jdk | 1.5.0 | update10    | All | All |
| Application | Sun | Jdk | 1.5.0 | update11    | All | All |
| Application | Sun | Jdk | 1.5.0 | update12    | All | All |
| Application | Sun | Jdk | 1.5.0 | update13    | All | All |
| Application | Sun | Jdk | 1.5.0 | update14    | All | All |
| Application | Sun | Jdk | 1.5.0 | update15    | All | All |
| Application | Sun | Jdk | 1.5.0 | update16    | All | All |
| Application | Sun | Jdk | 1.5.0 | update17    | All | All |
| Application | Sun | Jdk | 1.5.0 | update18    | All | All |
| Application | Sun | Jdk | 1.5.0 | update19    | All | All |
| Application | Sun | Jdk | 1.5.0 | update2     | All | All |
| Application | Sun | Jdk | 1.5.0 | update20    | All | All |
| Application | Sun | Jdk | 1.5.0 | update21    | All | All |
| Application | Sun | Jdk | 1.5.0 | update22    | All | All |
| Application | Sun | Jdk | 1.5.0 | update23    | All | All |
| Application | Sun | Jdk | 1.5.0 | update24    | All | All |
| Application | Sun | Jdk | 1.5.0 | update3     | All | All |
| Application | Sun | Jdk | 1.5.0 | update4     | All | All |
| Application | Sun | Jdk | 1.5.0 | update5     | All | All |
| Application | Sun | Jdk | 1.5.0 | update6     | All | All |
| Application | Sun | Jdk | 1.5.0 | update7     | All | All |
| Application | Sun | Jdk | 1.5.0 | update8     | All | All |
| Application | Sun | Jdk | 1.5.0 | update9     | All | All |
| Application | Sun | Jdk | 1.6.0 | All         | All | All |
| Application | Sun | Jdk | 1.6.0 | update1     | All | All |
| Application | Sun | Jdk | 1.6.0 | update1_b06 | All | All |
| Application | Sun | Jdk | 1.6.0 | update2     | All | All |
| Application | Sun | Jdk | 1.6.0 | update_10   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_11   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_12   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_13   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_14   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_15   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_16   | All | All |
| Application | Sun | Jdk | 1.6.0 | update_17   | All | All |

|             |     |     |       |           |     |     |
|-------------|-----|-----|-------|-----------|-----|-----|
| Application | Sun | Jdk | 1.6.0 | update_18 | All | All |
| Application | Sun | Jdk | 1.6.0 | update_19 | All | All |
| Application | Sun | Jdk | 1.6.0 | update_20 | All | All |
| Application | Sun | Jdk | 1.6.0 | update_3  | All | All |
| Application | Sun | Jdk | 1.6.0 | update_4  | All | All |
| Application | Sun | Jdk | 1.6.0 | update_5  | All | All |
| Application | Sun | Jdk | 1.6.0 | update_6  | All | All |
| Application | Sun | Jdk | 1.6.0 | update_7  | All | All |
| Application | Sun | Jdk | All   | update25  | All | All |
| Application | Sun | Jdk | All   | update_21 | All | All |
| Application | Sun | Jre | 1.5.0 | All       | All | All |
| Application | Sun | Jre | 1.5.0 | update1   | All | All |
| Application | Sun | Jre | 1.5.0 | update10  | All | All |
| Application | Sun | Jre | 1.5.0 | update11  | All | All |
| Application | Sun | Jre | 1.5.0 | update12  | All | All |
| Application | Sun | Jre | 1.5.0 | update13  | All | All |
| Application | Sun | Jre | 1.5.0 | update14  | All | All |
| Application | Sun | Jre | 1.5.0 | update15  | All | All |
| Application | Sun | Jre | 1.5.0 | update16  | All | All |
| Application | Sun | Jre | 1.5.0 | update17  | All | All |
| Application | Sun | Jre | 1.5.0 | update18  | All | All |
| Application | Sun | Jre | 1.5.0 | update19  | All | All |
| Application | Sun | Jre | 1.5.0 | update2   | All | All |
| Application | Sun | Jre | 1.5.0 | update20  | All | All |
| Application | Sun | Jre | 1.5.0 | update21  | All | All |
| Application | Sun | Jre | 1.5.0 | update22  | All | All |
| Application | Sun | Jre | 1.5.0 | update23  | All | All |
| Application | Sun | Jre | 1.5.0 | update24  | All | All |
| Application | Sun | Jre | 1.5.0 | update3   | All | All |
| Application | Sun | Jre | 1.5.0 | update4   | All | All |
| Application | Sun | Jre | 1.5.0 | update5   | All | All |
| Application | Sun | Jre | 1.5.0 | update6   | All | All |
| Application | Sun | Jre | 1.5.0 | update7   | All | All |
| Application | Sun | Jre | 1.5.0 | update8   | All | All |
| Application | Sun | Jre | 1.5.0 | update9   | All | All |

|             |     |     |       |           |     |     |
|-------------|-----|-----|-------|-----------|-----|-----|
| Application | Sun | Jre | 1.6.0 | All       | All | All |
| Application | Sun | Jre | 1.6.0 | update_1  | All | All |
| Application | Sun | Jre | 1.6.0 | update_10 | All | All |
| Application | Sun | Jre | 1.6.0 | update_11 | All | All |
| Application | Sun | Jre | 1.6.0 | update_12 | All | All |
| Application | Sun | Jre | 1.6.0 | update_13 | All | All |
| Application | Sun | Jre | 1.6.0 | update_14 | All | All |
| Application | Sun | Jre | 1.6.0 | update_15 | All | All |
| Application | Sun | Jre | 1.6.0 | update_16 | All | All |
| Application | Sun | Jre | 1.6.0 | update_17 | All | All |
| Application | Sun | Jre | 1.6.0 | update_18 | All | All |
| Application | Sun | Jre | 1.6.0 | update_19 | All | All |
| Application | Sun | Jre | 1.6.0 | update_2  | All | All |
| Application | Sun | Jre | 1.6.0 | update_20 | All | All |
| Application | Sun | Jre | 1.6.0 | update_3  | All | All |
| Application | Sun | Jre | 1.6.0 | update_4  | All | All |
| Application | Sun | Jre | 1.6.0 | update_5  | All | All |
| Application | Sun | Jre | 1.6.0 | update_6  | All | All |
| Application | Sun | Jre | 1.6.0 | update_7  | All | All |
| Application | Sun | Jre | All   | update25  | All | All |
| Application | Sun | Jre | All   | update_21 | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |  |
|-----------------------------------|--------|---------|--------------|---------------|--|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |  |

| References                                                                    |
|-------------------------------------------------------------------------------|
| Reference                                                                     |
| Repository / Oval Repository                                                  |
| SecurityFocus                                                                 |
| [SECURITY] Fedora 12 Update: java-1.6.0-openjdk-1.6.0.0-41.1.8.2.fc12         |
| Bug 642197 – CVE-2010-3567 OpenJDK ICU Opentype layout engine crash (6963285) |
| Support   Red Hat                                                             |
| USN-1010-1: OpenJDK vulnerabilities   Ubuntu                                  |
| Support   Red Hat                                                             |
| VMSA-2011-0003                                                                |

|                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------|
| [SECURITY] Fedora 14 Update: java-1.6.0-openjdk-1.6.0.0-44.1.9.1.fc14                                                                       |
| ASA-2010-347                                                                                                                                |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2010:019                                                                          |
| '[security bulletin] HPSBMU02799 SSRT100867 rev.1 - HP Network Node Manager i (NNMi) v9.0x Running JD' - MARC                               |
| [SECURITY] Fedora 13 Update: java-1.6.0-openjdk-1.6.0.0-43.1.8.2.fc13                                                                       |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                            |
| Oracle Java SE and Java for Business Critical Patch Update Advisory - October 2010                                                          |
| HPSBUX02608 SSRT100333 rev.2 - HP-UX Running Java, Remote Execution of Arbitrary Code, Disclosure of Information, and Other Vulnerabilities |
| Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities                                                                         |
| ASA-2010-308 (RHSA-2010-0768)                                                                                                               |
| Ubuntu update for openjdk - Advisories - Community                                                                                          |
| Repository / Oval Repository                                                                                                                |
| Oracle Critical Patch Update Pre-Release Announcement - January 2011                                                                        |
| Hitachi Products Multiple Vulnerabilities - Advisories - Community                                                                          |
| Oracle JRockit Multiple Vulnerabilities - Advisories - Community                                                                            |
| ASA-2010-307 (RHSA-2010-0770)                                                                                                               |
| Oracle Java SE and Java for Business CVE-2010-3567 Remote 2D Vulnerability                                                                  |
| rhn.redhat.com   Red Hat Support                                                                                                            |
| Cosminexusにおける複数の脆弱性：ソフトウェア製品セキュリティ情報：ソフトウェア：日立                                                                                             |
| CVE Program record                                                                                                                          |
| NVD vulnerability detail                                                                                                                    |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)