



# CVE-2015-7940

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

## Summary

<b>CVE</b>	CVE-2015-7940
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-11-09 16:59:00 UTC
<b>Updated</b>	2019-01-16 19:29:00 UTC
<b>Description</b>	The Bouncy Castle Java library before 1.51 does not validate a point is within the elliptic curve, which makes it easier for r

## Risk And Classification

**Problem Types:** CWE-310 | CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Bouncy Castle Crypto Package	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.1	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.2	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.3	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.1	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.2	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.3	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.1.4	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2.2	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.1.4	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2.2	All	All	All

Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.54	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.55	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.54	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.55	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Virtual Desktop Infrastructure</a>	3.5.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Virtual Desktop Infrastructure</a>	3.5.2	All	All	All

## References

### Reference

[Debian -- Security Information -- DSA-3417-1 bouncycastle](#)

[Red Hat Customer Portal](#)

[Oracle PeopleSoft Enterprise PeopleTools Multiple Flaws Let Remote Users Access and Modify Data on the Target System - SecurityTracker](#)

[Oracle Critical Patch Update - January 2018](#)

[CPU July 2018](#)

[Bouncy Castle CVE-2015-7940 Information Disclosure Vulnerability](#)

[Oracle Critical Patch Update - April 2018](#)

[\[SECURITY\] Fedora 22 Update: bouncycastle-1.50-8.fc22](#)

[oss-security - CVE Request: invalid curve attack on bouncycastle](#)

[Oracle Critical Patch Update - October 2016](#)

[Oracle Critical Patch Update - January 2019](#)

[On Web-Security and -Insecurity: Practical Invalid Curve Attacks](#)

[oss-security - Re: CVE Request: invalid curve attack on bouncycastle](#)

[Red Hat Customer Portal](#)

[\[security-announce\] openSUSE-SU-2015:1911-1: important: Security update](#)

[Oracle Enterprise Manager Bugs Let Remote Users Access Data and Local Users Access and Modify Data - SecurityTracker](#)

[Oracle VM VirtualBox Multiple Flaws Let Remote and Local Users Access and Modify Data and Let Local Users Deny Service and Gain Eleva](#)

[Oracle Critical Patch Update Advisory - April 2020](#)

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

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

[USN-3727-1: Bouncy Castle vulnerabilities | Ubuntu security notices | Ubuntu](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

981321 Java (maven) Security Update for org.bouncycastle:bcprov-jdk14 (GHSA-4mv7-cq75-3qjm)

© [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](#)