



# CVE-2018-2582

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

## Summary

<b>CVE</b>	CVE-2018-2582
<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>	2018-01-18 02:29:00 UTC
<b>Updated</b>	2023-11-21 19:13:00 UTC
<b>Description</b>	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versio

## 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="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp7 Command View</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp7 Command View</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp Command View</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp Command View</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp P9000 Command View</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Xp P9000 Command View</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jdk</a>	1.8.0	update152	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jdk</a>	1.9.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jdk</a>	9.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jdk</a>	1.8.0	update152	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jdk</a>	1.9.0.1	All	All	All

Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	1.8.0	<a href="#">update152</a>	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	1.8.0	<a href="#">update_152</a>	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	1.9.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	9.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	1.8.0	<a href="#">update_152</a>	All	All
Application	<a href="#">Oracle</a>	<a href="#">Jre</a>	1.9.0.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Satellite</a>	5.8	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Satellite</a>	5.8	All	All	All
Application	<a href="#">Schneider-electric</a>	<a href="#">Struxureware Data Center Expert</a>	All	All	All	All
Application	<a href="#">Schneider-electric</a>	<a href="#">Struxureware Data Center Expert</a>	All	All	All	All

## References

### Reference

[Document Display | HPE Support Center](#)

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

[Oracle Java SE CVE-2018-2582 Remote Security Vulnerability](#)

[Red Hat Customer Portal](#)


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

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

PGM 0

DCIM Support
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Debian -- Security Information -- DSA-4144-1 openjdk-8
USN-3613-1: OpenJDK 8 vulnerabilities   Ubuntu security notices
January 2018 Java Platform Standard Edition Vulnerabilities in NetApp Products   NetApp Product Security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
<b>Legacy QID Mappings</b>
<a href="#">710301</a> Gentoo Linux Oracle Java Development Toolkit/Java Runtime Error Multiple Vulnerabilities (GLSA 201803-06)

© [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](#)