



CVE-2018-2677

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-2677 |
| State | PUBLIC |
| Assigner | secalert_us@oracle.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-01-18 02:29:00 UTC |
| Updated | 2023-11-21 18:05:00 UTC |
| Description | Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 17.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 17.10 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Hp | Xp7 Command View | All | All | All | All |
| Application | Hp | Xp7 Command View | All | All | All | All |
| Application | Hp | Xp Command View | All | All | All | All |
| Application | Hp | Xp Command View | All | All | All | All |
| Application | Hp | Xp P9000 Command View | All | All | All | All |

| | | | | | | |
|------------------|--------|-----------------------------|---------|------------|-----|-----|
| Application | Hp | Xp P9000 Command View | All | All | All | All |
| Application | Oracle | Jdk | 1.6.0 | update171 | All | All |
| Application | Oracle | Jdk | 1.6.0 | update_171 | All | All |
| Application | Oracle | Jdk | 1.7.0 | update161 | All | All |
| Application | Oracle | Jdk | 1.8.0 | update152 | All | All |
| Application | Oracle | Jdk | 1.9.0.1 | All | All | All |
| Application | Oracle | Jdk | 9.0.1 | All | All | All |
| Application | Oracle | Jdk | 1.6.0 | update_171 | All | All |
| Application | Oracle | Jdk | 1.7.0 | update161 | All | All |
| Application | Oracle | Jdk | 1.8.0 | update152 | All | All |
| Application | Oracle | Jdk | 1.9.0.1 | All | All | All |
| Application | Oracle | Jre | 1.6.0 | update171 | All | All |
| Application | Oracle | Jre | 1.6.0 | update_171 | All | All |
| Application | Oracle | Jre | 1.7.0 | update161 | All | All |
| Application | Oracle | Jre | 1.7.0 | update_161 | All | All |
| Application | Oracle | Jre | 1.8.0 | update152 | All | All |
| Application | Oracle | Jre | 1.8.0 | update_152 | All | All |
| Application | Oracle | Jre | 1.9.0.1 | All | All | All |
| Application | Oracle | Jre | 9.0.1 | All | All | All |
| Application | Oracle | Jre | 1.6.0 | update_171 | All | All |
| Application | Oracle | Jre | 1.7.0 | update_161 | All | All |
| Application | Oracle | Jre | 1.8.0 | update_152 | All | All |
| Application | Oracle | Jre | 1.9.0.1 | 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 | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.6 | 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 | 7.4 | 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 | 7.4 | 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 | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.4 | 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 | Satellite | 5.6 | All | All | All |
| Application | Redhat | Satellite | 5.7 | All | All | All |
| Application | Redhat | Satellite | 5.8 | All | All | All |
| Application | Redhat | Satellite | 5.6 | All | All | All |
| Application | Redhat | Satellite | 5.7 | All | All | All |
| Application | Redhat | Satellite | 5.8 | All | All | All |
| Application | Schneider-electric | Struxureware Data Center Expert | All | All | All | All |
| Application | Schneider-electric | Struxureware Data Center Expert | All | All | All | All |

References

Reference

Red Hat Customer Portal

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

Red Hat Customer Portal

Debian -- Security Information -- DSA-4166-1 openjdk-7

Red Hat Customer Portal

Oracle Critical Patch Update - January 2018

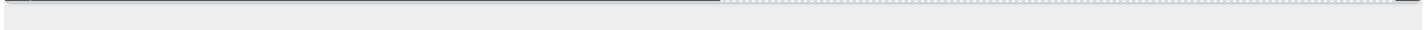
Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

| |
|--|
| DCIM Support |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| USN-3614-1: OpenJDK 7 vulnerabilities Ubuntu security notices |
| Red Hat Customer Portal |
| Debian -- Security Information -- DSA-4144-1 openjdk-8 |
| USN-3613-1: OpenJDK 8 vulnerabilities Ubuntu security notices |
| Oracle Java SE CVE-2018-2677 Remote Security Vulnerability |
| [SECURITY] [DLA 1339-1] openjdk-7 security update |
| Red Hat Customer Portal |
| 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.

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)