

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | Suppressing false positives | Getting Help: github issues

Project: project ':standalone'

pdfc:standalone:26.10

Scan Information (show all):

- *dependency-check version*: 13.0.0
- *Report Generated On*: Thu, 15 Oct 2026 20:04:40 +0200
- *Dependencies Scanned*: 135 (135 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 9 (show)
- ...

Summary

Summary of Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count

Dependencies (vulnerable)

Suppressed Vulnerabilities

ocr.tesseract.zip: jna.jar

Description:

JNA Library

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/standalone/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/jna.jar
MD5: 97fcb12698f8c1e4eed897e5c490e098
SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
Referenced In Project/Scope: standalone

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2009-2476 suppressed

The Java Management Extensions (JMX) implementation in Sun Java SE 6 before Update 15, and OpenJDK, does not properly enforce OpenType checks, which allows context-dependent attackers to bypass intended access restrictions by leveraging finalizer resurrection to obtain a reference to a privileged object.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513220
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513220
- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html

- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2689 suppressed

JDK13Services.getProviders in Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, grants full privileges to instances of unspecified object types, which allows context-dependent attackers to bypass intended access restrictions via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://java.sun.com/javase/6/webnotes/6u15.html
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html

- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2475 suppressed

Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, might allow context-dependent attackers to obtain sensitive information via vectors involving static variables that are declared without the final keyword, related to (1) LayoutQueue, (2) Cursor.predefined, (3) AccessibleResourceBundle.getContents, (4) ImageReaderSpi.STANDARD_INPUT_TYPE, (5) ImageWriterSpi.STANDARD_OUTPUT_TYPE, (6) the imageio plugins, (7) DnsContext.debug, (8) RmfFileReader/StandardMidiFileWriter.types, (9) AbstractSaslImpl.logger, (10) Synth.Region.uiToRegionMap/lowerCaseNameMap, (11) the Introspector class and a cache of BeanInfo, and (12) JAX-WS, a different vulnerability than CVE-2009-2673.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:N/AC:L/Au:N/C:C/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513215
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html

- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://java.sun.com/javase/6/webnotes/6u15.html
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513215
- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2716 suppressed

The plugin functionality in Sun Java SE 6 before Update 15 does not properly implement version selection, which allows context-dependent attackers to leverage vulnerabilities in "old zip and certificate handling" and have unspecified other impact via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460

- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2676 suppressed

Unspecified vulnerability in JNLPAppletlauncher in Sun Java SE, and SE for Business, in JDK and JRE 6 Update 14 and earlier and JDK and JRE 5.0 Update 19 and earlier; and Java SE for Business in SDK and JRE 1.4.2_21 and earlier; allows remote attackers to create or modify arbitrary files via vectors involving an untrusted Java applet that accesses an old version of JNLPAppletLauncher.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- af854a3a-2127-422b-91ae-364da2661108 - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- af854a3a-2127-422b-91ae-364da2661108 - http://osvdb.org/56789
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/bid/35946
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securitytracker.com/id?1022657
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - US_GOVERNMENT_RESOURCE
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- cve@mitre.org - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- cve@mitre.org - http://osvdb.org/56789
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.securityfocus.com/bid/35946
- cve@mitre.org - http://www.securitytracker.com/id?1022657
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH,VENDOR_ADVISORY
- cve@mitre.org - US_GOVERNMENT_RESOURCE
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:*:*:*:*:*:*:*
- ...

CVE-2009-2717 suppressed

The Abstract Window Toolkit (AWT) implementation in Sun Java SE 6 before Update 15 on Windows 2000 Professional does not provide a Security Warning Icon, which makes it easier for context-dependent attackers to trick a user into interacting unsafely with an untrusted applet.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2690 suppressed

The encoder in Sun Java SE 6 before Update 15, and OpenJDK, grants read access to private variables with unspecified names, which allows context-dependent attackers to obtain sensitive information via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2719 suppressed

The Java Web Start implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException) via a crafted .jnlp file, as demonstrated by the jnlp_file/appletDesc/index.html#misc test in the Technology Compatibility Kit (TCK) for the Java Network Launching Protocol (JNLP).

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2720 suppressed

Unspecified vulnerability in the javax.swing.plaf.synth.SynthContext.isSubregion method in the Swing implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException in the Jemmy library) via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460

- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - PATCH,VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the CISA Known Exploited Vulnerability Catalog.
This report may contain data retrieved from the Github Advisory Database (via NPM Audit API).
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype Guide OSS Index API.