

# [Full-disclosure] [ GLSA 200804-20 ] Sun JDK/JRE: Multiple vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-04/msg00479.html>

---

- *From:* Robert Buchholz <[rbu@xxxxxxxxxxx](mailto:rbu@xxxxxxxxxxx)>
  - *Date:* Fri, 18 Apr 2008 01:45:16 +0200
- 

-----  
Gentoo Linux Security Advisory GLSA 200804-20  
-----

<http://security.gentoo.org/>  
-----

Severity: Normal  
Title: Sun JDK/JRE: Multiple vulnerabilities  
Date: April 17, 2008  
Bugs: #178851, #178962, #183580, #185256, #194711, #212425  
ID: 200804-20  
-----

## Synopsis

=====

Multiple vulnerabilities have been identified in Sun Java Development Kit (JDK) and Java Runtime Environment (JRE).

## Background

=====

The Sun Java Development Kit (JDK) and the Sun Java Runtime Environment (JRE) provide the Sun Java platform.

## Affected packages

=====

-----  
Package / Vulnerable / Unaffected  
-----

```
1 dev-java/sun-jre-bin < 1.6.0.05 >= 1.6.0.05
  *>= 1.5.0.15
  *>= 1.4.2.17
2 dev-java/sun-jdk < 1.6.0.05 >= 1.6.0.05
  *>= 1.5.0.15
  *>= 1.4.2.17
```

3 app-emulation/emul-linux-x86-java < 1.6.0.05 >= 1.6.0.05  
\* >= 1.5.0.15  
\* >= 1.4.2.17

---

3 affected packages on all of their supported architectures.

---

## Description

=====

Multiple vulnerabilities have been discovered in Sun Java:

\* Daniel Soeder discovered that a long codebase attribute string in a JNLP file will overflow a stack variable when launched by Java WebStart (CVE-2007-3655).

\* Multiple vulnerabilities (CVE-2007-2435, CVE-2007-2788, CVE-2007-2789) that were previously reported as GLSA 200705-23 and GLSA 200706-08 also affect 1.4 and 1.6 SLOTS, which was not mentioned in the initial revision of said GLSAs.

\* The Zero Day Initiative, TippingPoint and John Heasman reported multiple buffer overflows and unspecified vulnerabilities in Java Web Start (CVE-2008-1188, CVE-2008-1189, CVE-2008-1190, CVE-2008-1191).

\* Hisashi Kojima of Fujitsu and JPCERT/CC reported a security issue when performing XSLT transformations (CVE-2008-1187).

\* CERT/CC reported a Stack-based buffer overflow in Java Web Start when using JNLP files (CVE-2008-1196).

\* Azul Systems reported an unspecified vulnerability that allows applets to escalate their privileges (CVE-2007-5689).

\* Billy Rios, Dan Boneh, Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and David Byrne discovered multiple instances where Java applets or JavaScript programs run within browsers do not pin DNS hostnames to a single IP address, allowing for DNS rebinding attacks (CVE-2007-5232, CVE-2007-5273, CVE-2007-5274).

\* Peter Csepely reported that Java Web Start does not properly enforce access restrictions for untrusted applications (CVE-2007-5237, CVE-2007-5238).

\* Java Web Start does not properly enforce access restrictions for untrusted Java applications and applets, when handling drag-and-drop operations (CVE-2007-5239).

\* Giorgio Maone discovered that warnings for untrusted code can be hidden under applications' windows (CVE-2007-5240).

- \* Fujitsu reported two security issues where security restrictions of web applets and applications were not properly enforced (CVE-2008-1185, CVE-2008-1186).
- \* John Heasman of NGSSoftware discovered that the Java Plug-in does not properly enforce the same origin policy (CVE-2008-1192).
- \* Chris Evans of the Google Security Team discovered multiple unspecified vulnerabilities within the Java Runtime Environment Image Parsing Library (CVE-2008-1193, CVE-2008-1194).
- \* Gregory Fleischer reported that web content fetched via the "jar:" protocol was not subject to network access restrictions (CVE-2008-1195).
- \* Chris Evans and Johannes Henkel of the Google Security Team reported that the XML parsing code retrieves external entities even when that feature is disabled (CVE-2008-0628).
- \* Multiple unspecified vulnerabilities might allow for escalation of privileges (CVE-2008-0657).

#### Impact

=====

A remote attacker could entice a user to run a specially crafted applet on a website or start an application in Java Web Start to execute arbitrary code outside of the Java sandbox and of the Java security restrictions with the privileges of the user running Java. The attacker could also obtain sensitive information, create, modify, rename and read local files, execute local applications, establish connections in the local network, bypass the same origin policy, and cause a Denial of Service via multiple vectors.

#### Workaround

=====

There is no known workaround at this time.

#### Resolution

=====

All Sun JRE users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose "dev-java/sun-jre-bin"
```

All Sun JDK users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose "dev-java/sun-jdk"
```

All emul-linux-x86-java users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose "app-emulation/emul-linux-x86-java"
```

#### References

=====

- [ 1 ] CVE-2007-2435  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2435>
- [ 2 ] CVE-2007-2788  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2788>
- [ 3 ] CVE-2007-2789  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2789>
- [ 4 ] CVE-2007-3655  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3655>
- [ 5 ] CVE-2007-5232  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5232>
- [ 6 ] CVE-2007-5237  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5237>
- [ 7 ] CVE-2007-5238  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5238>
- [ 8 ] CVE-2007-5239  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5239>
- [ 9 ] CVE-2007-5240  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5240>
- [ 10 ] CVE-2007-5273  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5273>
- [ 11 ] CVE-2007-5274  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5274>
- [ 12 ] CVE-2007-5689  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5689>
- [ 13 ] CVE-2008-0628  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0628>
- [ 14 ] CVE-2008-0657  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0657>
- [ 15 ] CVE-2008-1185  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1185>
- [ 16 ] CVE-2008-1186  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1186>
- [ 17 ] CVE-2008-1187  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1187>
- [ 18 ] CVE-2008-1188  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1188>
- [ 19 ] CVE-2008-1189  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1189>
- [ 20 ] CVE-2008-1190  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1190>
- [ 21 ] CVE-2008-1191  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1191>

[Full-disclosure] [ GLSA 200804-20 ] Sun JDK/JRE: Multiple vulnerabilities

[ 22 ] CVE-2008-1192

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1192>

[ 23 ] CVE-2008-1193

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1193>

[ 24 ] CVE-2008-1194

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1194>

[ 25 ] CVE-2008-1195

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1195>

[ 26 ] CVE-2008-1196

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1196>

[ 27 ] GLSA 200705-23

<http://www.gentoo.org/security/en/glsa/glsa-200705-23.xml>

[ 28 ] GLSA 200706-08

<http://www.gentoo.org/security/en/glsa/glsa-200706-08.xml>

#### Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200804-20.xml>

#### Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to [security@xxxxxxxxxx](mailto:security@xxxxxxxxxx) or alternatively, you may file a bug at <http://bugs.gentoo.org>.

#### License

=====

Copyright 2008 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.5>

#### ***Attachment: signature.asc***

*Description:* This is a digitally signed message part.

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>