Alpine Linux - Bug #7404

TLS negotiation error in OpenJDK 8 JRE u131

06/09/2017 07:44 AM - Shatil Rafiullah

Status:	Closed	**Start date:**	06/09/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	3.6.2		
Affected versions:	3.6.0, 3.6.1, 3.6.2	**Security IDs:**	

Description

Attempting to curl an application over HTTPS result in a TLS negotiation error with OpenSSL when the application is being served from Alpine Linux 3.6 running openjdk8-jre.

How to reproduce?

1. Launch Alpine Linux 3.6 container running a JVM application serving HTTPS
2. curl the application

```
$ curl -Ikv https://172.28.128.14/status
* Hostname was NOT found in DNS cache
*   Trying 172.28.128.14...
* Connected to 172.28.128.14 (172.28.128.14) port 443 (#0)
* successfully set certificate verify locations:
*   CAfile: none
  CApath: /etc/ssl/certs
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS alert, Server hello (2):
* error:14077438:SSL routines:SSL23_GET_SERVER_HELLO:tlsv1 alert internal error
* Closing connection 0
curl: (35) error:14077438:SSL routines:SSL23_GET_SERVER_HELLO:tlsv1 alert internal error
```

What version of Java am I running?

```
$ sudo docker exec -it docker_svc_1 java -version
openjdk version "1.8.0_131"
OpenJDK Runtime Environment (IcedTea 3.4.0) (Alpine 8.131.11-r1)
OpenJDK 64-Bit Server VM (build 25.131-b11, mixed mode)
```

Related bug in the OpenJDK Docker image project, which, according to its Dockerfile, just installs openjdk8-jre:
https://github.com/docker-library/openjdk/issues/115

curl from macOS Sierra doesn't complain, and neither does curl on Alpine Linux 3.6, but older (but supported) OSes like Ubuntu 14.04 are unable to communicate without issue. The issue does not exist in the same OpenJDK version running on Debian Jessie.

Associated revisions

Revision aba7b091 - 06/16/2017 12:17 PM - Shatil Rafiullah

community/openjdk8: Bug #7404 TLS negotiation error in OpenJDK 8 u131

Fixes an OpenJDK 8 regression discovered in docker-library/openjdk#115
on Alpine Linux 3.5 (u121) and 3.6 (u131) that causes TLS negotiation
errors for some clients.

Root cause appears to be OpenJDK announcing support for NIST curves the
underlying NSS library does doesn't. This patch limits OpenJDK's
announcement to elliptic curves 23 (secp256r1), 24 (secp384r1), and 25
(secp521r1).

Related issues:

- https://github.com/docker-library/openjdk/issues/115
- https://bugs.alpinelinux.org/issues/7404

- https://access.redhat.com/discussions/2339811
- https://bugzilla.redhat.com/show_bug.cgi?id=1022017
- https://bugzilla.redhat.com/show_bug.cgi?id=1348525

ref #7404

Revision a83deb21 - 06/16/2017 12:21 PM - Shatil Rafiullah

community/openjdk8: Bug #7404 TLS negotiation error in OpenJDK 8 u131

Fixes an OpenJDK 8 regression discovered in docker-library/openjdk#115
on Alpine Linux 3.5 (u121) and 3.6 (u131) that causes TLS negotiation
errors for some clients.

Root cause appears to be OpenJDK announcing support for NIST curves the
underlying NSS library does doesn't. This patch limits OpenJDK's
announcement to elliptic curves 23 (secp256r1), 24 (secp384r1), and 25
(secp521r1).

Related issues:

- https://github.com/docker-library/openjdk/issues/115
- https://bugs.alpinelinux.org/issues/7404
- https://access.redhat.com/discussions/2339811
- https://bugzilla.redhat.com/show_bug.cgi?id=1022017
- https://bugzilla.redhat.com/show_bug.cgi?id=1348525

ref #7404

Revision 0700bbb3 - 06/13/2018 09:18 PM - Shatil Rafiullah

community/openjdk8: Bug #7404 TLS negotiation error in OpenJDK 8 u131

Fixes an OpenJDK 8 regression discovered in docker-library/openjdk#115
on Alpine Linux 3.5 (u121) and 3.6 (u131) that causes TLS negotiation
errors for some clients.

Root cause appears to be OpenJDK announcing support for NIST curves the
underlying NSS library does doesn't. This patch limits OpenJDK's
announcement to elliptic curves 23 (secp256r1), 24 (secp384r1), and 25
(secp521r1).

Related issues:

- https://github.com/docker-library/openjdk/issues/115
- https://bugs.alpinelinux.org/issues/7404
- https://access.redhat.com/discussions/2339811
- https://bugzilla.redhat.com/show_bug.cgi?id=1022017
- https://bugzilla.redhat.com/show_bug.cgi?id=1348525

ref #7404

History

#1 - 06/09/2017 09:05 AM - Shatil Rafiullah

This appears to be a regression error. I think I've discovered the issue:
https://github.com/docker-library/openjdk/issues/115#issuecomment-307333336

Long story short, there is no ECDHE cipher suite supported in Alpine Linux 3.6's openjdk8-jre (u131). Support for these ciphers was present in Alpine Linux 3.4 (openjdk8-jre u111), and are also present in the Debian Jessie built of the OpenJDK Docker image.

Listed below are the cipher suites that Alpine 3.4's openjdk8-jre:

```
Testing ECDHE-RSA-AES256-GCM-SHA384...YES
Testing ECDHE-RSA-AES256-SHA384...YES
Testing ECDHE-RSA-AES256-SHA...YES
Testing DHE-RSA-AES256-GCM-SHA384...YES
Testing DHE-RSA-AES256-SHA256...YES
Testing DHE-RSA-AES256-SHA...YES
Testing AES256-GCM-SHA384...YES
Testing AES256-SHA256...YES
Testing AES256-SHA...YES
Testing ECDHE-RSA-DES-CBC3-SHA...YES
Testing EDH-RSA-DES-CBC3-SHA...YES
Testing DES-CBC3-SHA...YES
```

```
Testing ECDHE-RSA-AES128-GCM-SHA256...YES
Testing ECDHE-RSA-AES128-SHA256...YES
Testing ECDHE-RSA-AES128-SHA...YES
Testing DHE-RSA-AES128-GCM-SHA256...YES
Testing DHE-RSA-AES128-SHA256...YES
Testing DHE-RSA-AES128-SHA...YES
Testing AES128-GCM-SHA256...YES
Testing AES128-SHA256...YES
Testing AES128-SHA...YES
```

#2 - 06/14/2017 01:32 AM - Shatil Rafiullah

Explanation: https://github.com/docker-library/openjdk/issues/115#issuecomment-308293127

tl;dr: NSS supports only *some* NIST elliptic curves, but OpenJDK lists everything that SunEC supports, regardless of what the underlying deps may or may not support.

Possible solution: http://icedtea.classpath.org//hg/icedtea?cmd=changeset;node=04327567ef0a

```
diff --git a/SupportedEllipticCurvesExtension.java b/SupportedEllipticCurvesExtension.java
index 59f4b74..75695c6 100644
--- a/SupportedEllipticCurvesExtension.java
+++ b/SupportedEllipticCurvesExtension.java
@@ -183,6 +183,10 @@ final class SupportedEllipticCurvesExtension extends HelloExtension {
                 };
             }

+            // NSS currently only supports these three NIST curves
+            ids = new int[] {
+                23, 24, 25,
+            };
             idList = new ArrayList<>(ids.length);
             for (int curveId : ids) {
                 if (isAvailableCurve(curveId)) {
```

It's probably smarter to patch isAvailableCurve so it's truthful....

#3 - 06/14/2017 11:56 PM - Shatil Rafiullah

- File icedtea-jdk-tls-nist-curves.patch added

Solution attached as a patch. I tested it and found the same ciphers as Alpine Linux 3.4 also show up again, and I have no client-side issues communicating with the JVM service.

I don't know if you want a diff as well for APKBUILD, but here it is:

```
diff --git a/community/openjdk8/APKBUILD b/community/openjdk8/APKBUILD
index 4f8db316d5..3c15df779e 100644
--- a/community/openjdk8/APKBUILD
+++ b/community/openjdk8/APKBUILD
@@ -66,6 +66,7 @@ source="http://icedtea.classpath.org/download/source/icedtea-$_icedteaver.tar.gz
        icedtea-jdk-includes.patch
        icedtea-jdk-getmntent-buffer.patch
        icedtea-autoconf-config.patch
+       icedtea-jdk-tls-nist-curves.patch
        "
 builddir="$srcdir/icedtea-$_icedteaver"

@@ -286,4 +287,5 @@ b135991c76b0db8fa7c363e0903624668e11eda7b54a943035c214aa4d7fc8c3e8110ed200edcec8
 cdebe2c59657e7fd317a4841b2fbe95d9e8d7ee9d1593edf352ed7f49a92a42cbce82cbaa404d3f02c6d273eae03222a79559c09bf6cf
439396c5ec5434f5458  icedtea-jdk-musl.patch
 e8d9f1b867bf4fc84aa00d1237b264bcf503b1ed5f34735e14b0b747a728953fe0051a5af69ed058d377fbf65d8be1ed9e38fe5fc6edb
2d50b31f34bf3ba91dc  icedtea-jdk-includes.patch
 7e6fa46b10c630517bfa46943858aea1d032c12d32ba3fcb7a2143ae1e896c34fa4cb8f925af80cb19f8e29149b835aa054adfd30ebb0
0539f6c78588d6f5211  icedtea-jdk-getmntent-buffer.patch
-662d662d0a7a84be2978e921317589f212f3ba3b7629527ba0f1140b5ac4c1024893e0ed176211688ed1a4505968c4befc841ed57ffcd
bb9d355c2cb0571b167  icedtea-autoconf-config.patch"
+662d662d0a7a84be2978e921317589f212f3ba3b7629527ba0f1140b5ac4c1024893e0ed176211688ed1a4505968c4befc841ed57ffcd
bb9d355c2cb0571b167  icedtea-autoconf-config.patch
+105d5b05b5783d731d40976e1df552176caf98f067697b2b4bd873e66551ac2bad4972aa0fd2ad9a7e65b396de603833165715560eb8a
264da99aa6ce2682782  icedtea-jdk-tls-nist-curves.patch"
```

Further explanation: https://github.com/docker-library/openjdk/issues/115#issuecomment-308562429

What do I do to get this merged in?

#4 - 06/15/2017 05:16 PM - Shatil Rafiullah

Pull request: https://github.com/alpinelinux/aports/pull/1697

#5 - 06/16/2017 11:38 AM - Natanael Copa

- Target version set to 3.6.2

#6 - 06/16/2017 02:27 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

#7 - 06/16/2017 03:02 PM - Natanael Copa

- Status changed from Resolved to Closed

Files

icedtea-jdk-tls-nist-curves.patch	1.81 KB	06/14/2017	Shatil Rafiullah